UNITED STATES DISTRICT COURT
FOR THE DISRICT OF COLUMBIA

BROIDY CAPITAL MANAGEMENT LLC
1801 Century Park East, Suite 2150
Los Angeles, CA 90067

and

ELLIOTT BROIDY,
1801 Century Park East, Suite 2150
Los Angeles, CA 90067

Plaintiffs,

v.

NICOLAS D. MUZIN,
800 Stonington Rd.
Silver Spring, MD 20902-1552

JOSEPH ALLAHAM,
114 E 71st St., Apt. 7E
New York, NY 10021-5058

GREGORY HOWARD,
12 Moses Ln.
Phippsburg, ME 04562-5047

and

STONINGTON STRATEGIES LLC
550 Madison Avenue
New York, NY 10022

Defendants.

Civil Action No. _____

COMPLAINT AND JURY DEMAND

PUBLIC VERSION

PLAINTIFFS BROIDY CAPITAL MANAGEMENT AND ELLIOTT BROIDY'S COMPLAINT AND JURY DEMAND

Plaintiffs Broidy Capital Management and Elliott Broidy, by and through their undersigned counsel, bring this action seeking monetary damages and equitable relief against Defendants Nicolas D. Muzin ("Muzin"), Joseph Allaham ("Allaham"), Gregory Howard

("Howard"), and Stonington Strategies LLC ("Stonington") for their unlawful conduct, as set forth below.

INTRODUCTION

1. Elliott Broidy is a private businessman who has long been a critic of countries that fund and harbor terrorists. The Department of Homeland Security asked Mr. Broidy to be a member of the Homeland Security Advisory Council, where he served from 2006 to 2009. In that capacity, he contributed to the report of the Council's Future of Terrorism Task Force, which called for the elimination of terrorist safe havens throughout the world. Mr. Broidy's concerns led him in recent years to become an outspoken critic of the State of Qatar, which he publicly criticized for funding terrorist organizations and which he worked to expose as a negative influence in the Middle East. Mr. Broidy's work has helped bring significant public condemnation to Qatar, including from the President of the United States and several Congressional leaders. Mr. Broidy's work consequently drew the ire of Qatar and its paid agents in the United States, which, in 2017, flagged him as a major thorn in Qatar's side.

2. This case is about a criminal conspiracy to retaliate against, discredit, and ultimately silence Mr. Broidy. It is a stunning, true story of an international criminal racketeering enterprise and tortious conspiracy, funded by Qatar and orchestrated by a high-ranking, former U.N. diplomat and his highly paid U.S. co-conspirators, including named Defendants here (collectively, the "Qatari Enterprise"), which unlawfully targeted Mr. Broidy solely because of his successful efforts to call public attention to Qatar's support of Hamas, al Qaeda, the Muslim Brotherhood and a host of other international terrorist organizations.

3. Plaintiffs Elliott Broidy and his primary business, Broidy Capital Management LLC (collectively, "Broidy" or "Plaintiffs") bring this action under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), as well as other federal and state causes of action, to

remedy and prevent serious business and property injury by reason of, and invasion of privacy and other harms caused by, Defendants' participation in this far-flung racketeering enterprise and tortious conspiracy.

4. The Qatari Enterprise began as an unscrupulous, dark-money political operation designed to rehabilitate Qatar's tainted diplomatic reputation around the world and tarnish the reputations of those it considers enemies. But it ultimately crossed a line in violation of the common law and federal and state statutes in the way in which it targeted Mr. Broidy. Its scheme against Plaintiffs stretches from Qatar and the Middle East into the United States, corrupting seemingly legitimate lobbying organizations and foreign agents, both registered and unregistered.

5. Defendants and their co-conspirators engaged in a scheme of extortion, illegal hacking, and unlawful distribution of carefully curated batches of Plaintiffs' private documents. They used shell companies to mask payments and transactions that crossed international and state lines, they covered their tracks with incomplete, untimely and at times false federal lobbying disclosures, and they engaged in a pattern of cyber hacking and disinformation schemes against numerous political opponents that continues today. The overarching goal has been to silence Mr. Broidy by destroying his credibility, damaging his business, causing financial harm, and, as one Defendant stated to another, putting Plaintiffs "in Mueller's crosshairs."

6. Defendants here—Nicolas Muzin, Joseph Allaham, and Gregory Howard—were key participants in this unlawful enterprise. They enabled, facilitated, and participated in the conspiracy and criminal enterprise to target and unlawfully harm Mr. Broidy and his business. They sought to extort Mr. Broidy's close associate in an effort to get him to turn on Mr. Broidy and aid the criminal enterprise. They actively and knowingly participated in the deceptive

curation and distribution of stolen material to media organizations and pliable journalists, and they took credit for the success of the scheme in harming Plaintiffs on behalf of Qatar.

7. [redacted]

8. Defendants collectively and individually were paid millions of dollars by Qatar, its agents, and its instrumentalities to participate in the conspiracy to disseminate hacked materials and join the Qatari Enterprise. They interfered with, and injured, the privacy interests, business, and property of Plaintiffs.

9. Defendants aimed specifically to silence Mr. Broidy, punish and suppress his political expression, alienate him in U.S. foreign policy circles, and reduce his influence on United States foreign policy—all in an effort to remove him as an obstacle to Qatar's efforts to improve its public relations standing in the United States and abroad. They sought to do so by manufacturing negative news stories, exposing his confidential communications and trade secrets to the public, and, in so doing, damaging his business relationships and public standing.

10. The damage caused by the Qatari Enterprise is vast and far-reaching. Since at least 2014, the enterprise has targeted and hacked more than 1,400 email addresses belonging to a range of high-profile figures in government, business, journalism, and human rights advocacy in the United States, Europe, the Middle East and elsewhere around the world. Dozens of United States citizens and organizations have been targeted, including former intelligence officials, former staffers from the Democratic National Committee and the Hilary Clinton Presidential campaign, high-profile political activists opposed to the Assad regime in Syria, and a researcher

at a Washington, D.C., think tank currently investigating foreign influence in the 2016 elections. Other notable individuals targeted include FIFA soccer stars, former European defense officials, South Indian film actors and actresses, and hundreds of government leaders and diplomats across the Middle East.

11. Plaintiffs are entitled to relief from Defendants' unlawful conduct, as described below.

PARTIES

12. Plaintiff Broidy Capital Management LLC ("BCM") is an investment firm run by Elliott Broidy. BCM is a single-member, limited liability company duly organized under the laws of the State of California with its principal place of business in Los Angeles, California. Mr. Broidy is the sole member of BCM and resides in California.

13. Plaintiff Elliott Broidy is a citizen of the United States and the State of California who resides in Los Angeles, California. He is the Chief Executive Officer and Chairman of BCM. Plaintiff Broidy is a prominent business and civic leader and philanthropist who has actively served in leadership roles in the Republican Party and Jewish organizations, including the Simon Wiesenthal Center. His advocacy against terrorism and extremism, and in protection of his country, is well known, as is his criticism of Qatar for sponsoring terrorism.

14. Defendant Nicolas D. Muzin is a citizen of the United States and a resident of Maryland. Muzin has regularly conducted business and political operations in Washington D.C. during recent years, including working as Chief Executive Officer of Stonington Global LLC (formerly known as "Stonington Strategies"), a consulting firm based in Washington D.C. In that capacity he works as a political lobbyist and, from 2017 until at least August of 2018, was a registered foreign agent of Qatar. Muzin was dismissed for lack of personal jurisdiction from

related litigation brought by Plaintiffs in the United States District Court for the Central District of California.

15. Muzin is a high-level Republican political operative. He served as chief of staff to then-Congressman (now Senator) Tim Scott and later as deputy chief of staff for strategy to Senator Ted Cruz. Muzin worked on the Presidential campaign of Donald J. Trump, as well as on the transition team to recruit candidates for the new administration. Shortly after President Trump's inauguration, Muzin began working as a lobbyist, first registering under the Foreign Agents Registration Act ("FARA"), 22 U.S.C. § 611 *et seq.*, as an agent for the Democratic Party of Albania in March 2017. On August 24, 2017, he was retained by Qatar for consulting services.

16. Starting in September 2017, Muzin helped spearhead Qatar's outreach to the Republican Jewish community in the United States, which in general tends to be politically conservative and pro-Israel. The substantial money he received from Qatar corrupted Muzin and Stonington Strategies, and he crossed the legal line from being a legitimate political operative working on behalf of a foreign government into becoming a member of a criminal enterprise and conspiracy.

17. Defendant Joseph Allaham is a resident of New York and the co-founder of Stonington Strategies, where he serves as partner and frequently conducts business in Washington D.C. He was also a prominent owner of several now-defunct restaurants and has worked for Qatar, originally as an unregistered foreign agent until he belatedly filed a registration statement under FARA on June 15, 2018, in response to a subpoena from Plaintiffs in a related action.

18. Defendant Gregory Howard is a resident of Maine and a media placement expert who in 2017 and 2018 worked as a Vice President and Senior Media Strategist at the firm of Conover & Gould ("Conover"), based in Washington D.C. From July 2017 until January 18, 2018, Greg Howard was a registered foreign agent of Qatar through Conover. He currently works in Washington D.C. as Vice President of Mercury Public Affairs, a public strategy firm. For both companies, he worked as a media placement strategist for Qatar. At all times relevant to this suit, Defendant Howard worked and conducted business within Washington D.C.

19. Defendant Stonington Strategies LLC ("Stonington") is a public relations and lobbying firm organized under the laws of Delaware. It was founded by Defendants Muzin and Allaham. Upon information and belief, no member of Stonington is a resident of California. Stonington's principal place of business is Washington D.C. On September 3, 2017, Stonington registered under FARA as a foreign agent providing "strategic communications" for the State of Qatar. Stonington, like Muzin, was dismissed for lack of personal jurisdiction from related litigation brought by Plaintiffs in the United States District Court for the Central District of California.

JURISDICTION

20. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331. A number of Plaintiffs' claims arise under federal law, including under the RICO Act (Counts One and Two); the Stored Communications Act (Count Three); the Computer Fraud and Abuse Act (Count Four); the misappropriation of trade secrets under the Defend Trade Secrets Act and the Economic Espionage Act (Count Five).

21. This Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over Plaintiffs' other claims since those other claims relate to the federal statutory claims in this

action and form part of the same case or controversy under Article III of the United States Constitution.

22. Additionally, this Court has diversity subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because Plaintiffs and Defendants are from different states and the amount in controversy exceeds $75,000, exclusive of interest and costs.

23. All Defendants are citizens of the United States and therefore are subject to its jurisdiction without recourse to any foreign or diplomatic immunity. Even if they could assert derivative sovereign immunity (which does not apply), this Court has jurisdiction pursuant to 28 U.S.C. § 1605(a)(2) and (a)(5).

24. This Court has personal jurisdiction over all Defendants. Defendants Muzin and Allaham regularly conduct business out of Stonington's principal place of business in its Washington D.C. office. In all actions relevant to this Complaint, Muzin and Allaham acted as principals of Stonington. Defendant Stonington regularly conducts business in Washington D.C.

25. Defendant Howard was at all times relevant to this Complaint employed by at least one or both of Conover & Gould in Washington D.C., and Mercury Public Affairs in Washington D.C., both of which have Washington D.C. as their principal place of business. Howard regularly contacted journalists and media organizations in Washington D.C. and transacted business with numerous subcontractors and outside public relations firms in the District to further the conspiracy.

26. Defendants all have continuous and systematic contacts with this judicial district. They have purposefully availed themselves of the privilege of conducting activities in Washington D.C. and have enduring contacts in the District. Stonington's principal place of business, where both Muzin and Allaham worked, is Washington D.C. *See* D.C. Code § 13-422.

27. This lawsuit arises out of Defendants' business transacted in this judicial district. *See* D.C. Code § 13-423(a). Defendants committed several tortious acts in Washington D.C. that were in furtherance of the Qatari Enterprise and that injured Plaintiffs in this District—including, but not limited to, contacting media organizations and journalists in Washington, D.C. to disseminate false and misleading stories based on the hacked and stolen information about Broidy.

28. Defendants conspired in Washington, D.C. to disseminate carefully selected stolen information from the hacks to harm Broidy. These tortious acts harmed Broidy's standing and business relationships in Washington, D.C. and thus caused Plaintiffs substantial injury. Defendants' suit-related conduct thereby created a substantial connection with the District of Columbia.

29. Moreover, this Court has personal jurisdiction over all Defendants because they joined in a conspiracy against Broidy, during which Defendants committed several overt acts in furtherance of the conspiracy in Washington, D.C. For example, Defendant Muzin met three times with an associate of Mr. Broidy in Washington, D.C. to make threats and extort Plaintiffs into doing the bidding of the Qatari Enterprise. This overt act grants this Court personal jurisdiction over every Defendant in the conspiracy.

VENUE

30. Venue is proper under 18 U.S.C. § 1965(a) because at least one Defendant transacts his affairs in this District.

31. Venue is also proper under 28 U.S.C. § 1391(b)(2) because this is a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred. Defendants conspired together and coordinated their illegal campaign to discredit and injure Plaintiffs in Washington, D.C.

32. Alternatively, venue is proper in this judicial district under 28 U.S.C. § 1391(b)(3) because there is no state in which all non-foreign defendants are resident, and at least one Defendant is subject to personal jurisdiction in the District of Columbia.

FACTS

33. This case concerns a racketeering conspiracy undertaken by members of a criminal enterprise against an influential United States citizen and his primary business. Defendants targeted Plaintiffs on behalf of Qatar because Mr. Broidy spoke out forcefully and effectively against Qatar's support for terrorism and against its efforts to relieve economic sanctions against it.

34. Defendants participated in tortious, illegal means to thwart Mr. Broidy's exercise of his First Amendment rights within the United States through a campaign (1) to discredit him through the press and in the eyes of U.S. government officials, and (2) to interfere in and disrupt Plaintiffs' business relationships. The conspiracy included the commissioned hacking of Plaintiffs' computer networks, including Plaintiffs' email accounts, and distribution of curated batches of the illegally obtained data to the media in a manner calculated to create a false and injurious image of Mr. Broidy.

35. Defendants' role in this criminal enterprise included identifying Mr. Broidy as a target of the Qatari Enterprise, and then knowingly receiving stolen information from the illegal cyberattacks, carefully curating that information to create damaging stories about Broidy, and disseminating that stolen information to the media and favorable journalists. Defendant Muzin was also a key player in seeking to extort a close associate of Mr. Broidy in order to pressure him into changing sides in favor of Qatar.

36. At all times relevant to this Complaint, Qatar had been subjected to international sanctions because of its support for terrorism. Defendants were paid millions of dollars by

Qatar, and/or its affiliated entities, to improve Qatar's image in the United States and to target its enemies in the United States, including American citizens. Defendants specifically targeted Plaintiffs and participated in a conspiracy to disseminate stolen, confidential emails and other confidential information to the media as part of an effort to punish Plaintiffs and silence their criticism of Qatar through a sustained and ongoing pattern of racketeering.

I. Qatar is Sanctioned For Supporting Terrorism.

37. Qatar provides sanctuary for terrorist leaders and organizations, including but not limited to Al Qaeda (and its affiliates including Al-Shabab and Al Qaeda in Syria, also known as Al-Nusra Front or Jabhat Al-Nusra), Hamas, the Taliban, and the Muslim Brotherhood.

38. Qatar has allied itself in close strategic partnership with regimes governing Iran and Russia.

39. Numerous individuals residing in Qatar have been sanctioned by the United States Department of Treasury for raising funds for Al Qaeda.

40. Qatar also has permitted Hamas leaders to operate freely within the country. Indeed, Qatar has provided substantial funding to Hamas, despite being subjected to the threat of international political and economic sanctions for such support.

41. Qatar has further allowed the Taliban to operate and maintain an office in Doha since at least 2014.

42. Qatar has given safe haven to many leaders of the Muslim Brotherhood after their expulsion from Egypt by the Egyptian government.

43. On June 5, 2017, several neighboring Middle Eastern states severed diplomatic relations with Qatar and imposed an economic blockade and embargo against the country because of its support for terrorism and its close ties to Iran. Several other governments soon did the same. Some countries closed their airspaces to Qatari aircraft, closed their borders with

Qatar, and/or banned Qatari-flagged ships from docking at their ports. The sanctioning states issued a set of demands to Qatar, including that it curb ties with Iran and stop funding terrorist organizations. Qatar has rejected those demands.

44. The international sanctions, supported by the United States, threatened to damage the income of Qatari's ruling families, as well as harm its reputation and consequently erode the influence Qatar had painstakingly built up over the past two decades. The sanctioning states threatened to expel Qatar from the Gulf Cooperation Council, a regional economic and security cooperation body made up of six nations. The economic quarantine led to a significant drop-off in foreign investment in Qatar. According to the International Monetary Fund, "following the rift, foreign financing (non-resident deposits and inter-bank placements) and resident private-sector deposits fell by about US$40 billion."

45. These international sanctions on Qatar remain in effect today.

II. Elliott Broidy Criticizes Qatar's Sponsorship of Terrorism.

46. Plaintiff Elliott Broidy is a prominent business and civic leader who has actively served in leadership roles in U.S. government advisory groups, Jewish organizations, and the Republican Party for decades. During pertinent periods, he directly interacted with the President of the United States. His advocacy against terrorism and extremism is well known. Mr. Broidy served on the Homeland Security Advisory Council from 2006 to 2009 and specifically on the Future of Terrorism Task Force of that Council. The Task Force issued a report on January 11, 2007, that found, "Factors that will influence the future of terrorism include: the leadership of the terrorists, US counterterrorism efforts, status of political reform in Muslim nations and the elimination of safe havens[.]" This report was directed at and, was known to, countries operating as safe havens for terrorist organizations, including Qatar.

47. Beginning in early 2017, Mr. Broidy became a vocal critic of Qatar's support for terrorists and friendly relationship with Iran, which he sees as a major threat to the security of the United States and its allies. His efforts have succeeded in generating opposition to Qatar's efforts to whitewash its support for terrorist organizations.

48. Since that time, as a private citizen, Mr. Broidy has regularly conveyed his criticism of Qatar in meetings with United States officials and civic leaders, and on the issue of Qatari terrorism, he directly conferred with the President of the United States.

49. In the early days of the new administration, Qatar became concerned about the President's position towards it. Qatari officials complained in particular about the President's remarks at a June 2017 meeting of the Republican National Committee in which he criticized Qatar: "We're having a dispute with Qatar—we're supposed to say Qatar. It's Qatar, they prefer. I prefer that they don't fund terrorism."

50. At the same meeting, the President of the United States publicly identified Mr. Broidy in the audience and stated: "Elliott Broidy is fantastic." That acknowledgment was followed by a round of applause.

III. Defendants Join the Qatari Enterprise.

51. The chief goals of the Qatari Enterprise were to (1) improve Qatar's reputation in the United States, (2) end the blockade and sanctions against Qatar, and (3) improve Qatar's standing in the world and the global marketplace—without having to forgo their support for terrorism or break their close ties with Iran. A central component of that strategy was a multi-million dollar dark money effort to recruit lobbyists and influencers to polish Qatar's public image within the United States. That effort sought to use Republican lobbyists like Muzin who worked on the Trump campaign to influence American public opinion and the Trump Administration.

52. As part of this effort, Qatar retained Defendants with a specific plan of trying to influence the Republican, American Jewish community and other conservative supporters of Israel. The ultimate objective of this public relations effort was to co-opt this key constituency of the current President of the United States to reverse or neutralize the Trump Administration's position on Qatar.

53. These broad objectives are not illegal on their face. But they were pursued, in large part, through illegal conduct. What once may have been a public relations effort quickly crossed the line into a pattern of criminal racketeering and other tortious conduct to silence the critics of Qatar, most notably Mr. Broidy. Defendants were deeply involved in this unlawful activity, including knowingly disseminating emails and documents hacked and stolen from Broidy to the U.S. media in an effort to destroy Broidy's public standing, as well as efforts to extort a longtime associate of Mr. Broidy to join in their conspiracy, as described below.

A. Defendants Muzin and Allaham Officially Begin Work For Qatar.

54. In the fall of 2017, both Muzin and Allaham joined forces in the Qatari Enterprise with Jamal Benomar, a dual citizen of Morocco and the United Kingdom and former high-ranking United Nations official who resigned from his position at the United Nations on July 1, 2017, and shortly thereafter entered into a lucrative consultancy for Qatar and became a high-level member of the Qatari Enterprise. Benomar has resided in the United States for more than 20 years. [redacted]

55. Benomar coordinated payments from Qatar to Muzin and Allaham, acting on behalf of the Qatari Enterprise. In fact, Allaham testified under oath in a related proceeding that he had contemplated suing Benomar for five to ten million dollars that he believed Qatar owed

him, but decided not to do so only because he believed that Benomar had stashed the millions "offshore."

56. Muzin began working for Qatar sometime in 2017. In late August 2017, the Qatari Embassy in Washington, D.C., officially retained Stonington and Muzin to influence public opinion regarding Qatar. Their agreement specified that Muzin and Stonington were to provide "consulting services" including the "development and implementation of a government relations strategy for Qatar, as requested and directed by the Embassy." The initial agreement that Defendant Muzin submitted to the Department of Justice provided that Qatar would pay Muzin and Stonington Strategies $50,000 a month for these services.

57. Defendant Allaham began working for Qatar in 2017—according to his initial FARA disclosures in his capacity as the CEO of Lexington Strategies. According to his (belatedly filed) FARA registration, he worked directly for the Emir of Qatar, Sheikh Tamim bin Hamad Al Thani, and his brother Sheikh Mohamad bin Hamad Al Thani. The Emir's brother is commonly referred to as "MBH."

58. [redacted]

59. Defendants knew, or should have known, that their contacts within the Qatari government had a history of corrupt practices based on the well-known and reported efforts by Qatar to win its bid for the 2022 FIFA World Cup.

60. MBH was the chair of an organization that helped to manage Qatar's 2022 FIFA World Cup bid, the Supreme Committee for Delivery and Legacy. The Qatari bid for the World

Cup was beset by corruption and led to the United States investigation and prosecution of FIFA, the international governing body of soccer. More than a dozen individuals have been convicted of or pleaded guilty to criminal charges related to the corrupt bid.

61. According to media accounts, the "black ops" team that carried out the "dirty tricks" campaign that played the critical role in winning its tainted World Cup bid was overseen by Ahmad Nimeh, who is a key figure behind the secretive entity (discussed below) that Defendant Muzin belatedly claimed in his October 2018 FARA disclosure had paid him and Allaham $3.9 million more than a year earlier.

62. MBH's chief of staff at all times relevant to this Complaint was Ali al-Thawadi ("al-Thawadi"), who not only had assisted MBH with his corrupt efforts to obtain the World Cup, but also had direct contacts with Allaham and Benomar.

63. Allaham was paid at least $1.45 million by Qatar. Allaham stated in his FARA filing that the large payment was an "initial grant" for "compensation, disbursements, and operating expenses" for his efforts "to promote, the 2022 World Cup in Qatar." In his deposition, [redacted]

64. Starting on November 20, 2017 and continuing through the end of the month, Benomar had extensive telephone and text interaction with al-Thawadi. During this exact same time frame in late November 2017, Benomar also had at least seven phone calls and text message communications with Allaham, who stated in his FARA filings that his direct point of contact for his Qatar work was al-Thawadi, and that he worked with MBH.

65. Allaham and al-Thawadi exchanged five phone calls from late October through mid-November 2017, [redacted]

66. In November 2017, Benomar engaged in extensive communications with al-Thawadi, MBH's chief of staff. These communications indicate that both Benomar and Allaham, who reported on his FARA disclosure that he worked with MBH, were communicating directly with the highest members of the Qatari government.

67. [redacted]

68. Allaham later denied that he had an offshore account in his deposition testimony, even though his phone records reveal more than 40 calls with a Caribbean offshore bank, the Bank of Nevis International, between February and March of 2018. When questioned about these numerous calls in his deposition, Allaham stated he called the bank to inquire about opening an account.

69. [redacted]

70. In legal filings, Benomar belatedly claimed a year after the fact to have been a diplomat for the Moroccan mission to the United Nations from November 2017 until the present.

B. Allaham and Muzin's services to Qatar expanded to include reaching out to the Jewish community in the United States.

71. Qatar's desire was to influence the President of the United States, who had been publicly critical of Qatar. To accomplish that objective, Qatar embarked on a strategy to reach out to, and engage with, a strong constituency of the President, the Republican Jewish community, which is predisposed to be interested in Middle-East affairs because of the community's almost universal support for Israel. As a former Trump campaign official, Muzin was useful to the Qatari's cause.

72. On November 2, 2017, Allaham paid $50,000 to the Zionist Organization of America ("ZOA") in furtherance of his efforts to influence the conservative-segment of the American Jewish community to favor Qatar, according to disclosures in his belated FARA registration in June 2018.

73. Allaham spent the $50,000 to purchase a VIP table at ZOA's annual gala in New York City in November 2017, where Allaham's guest was the former head of Qatar Investments, Ahmed Al-Rumaihi ("Al-Rumaihi"). Qatar Investments was a U.S.-based subsidiary of the Qatar Investment Authority ("QIA"), the primary sovereign investment fund of Qatar.

74. Allaham, however, failed to register under FARA for any of these activities on behalf of Qatar until he was publicly unmasked in a related litigation. On June 6, 2018, Judge Katherine Forrest of the Southern District of New York granted Plaintiffs' motion to compel the production of documents from Allaham in a subpoena-enforcement action. On the same day as Judge Forrest's decision, Allaham issued a statement to the media, published early the next morning, announcing that he would belatedly register under FARA as a foreign agent of Qatar.

75. Allaham has never filed a Supplemental Statement, which is required within 30 days of the end of the first six months of work as a foreign agent, nor has he filed a formal

termination of his status as a foreign agent for Qatar. His registration says nothing about helping Qatar to end the blockade against it.

76. Muzin's and Allaham's efforts to influence the Republican, American Jewish community were largely ineffective, in part because of Mr. Broidy's actions to undercut any efforts by Qatar, a state-sponsor of terror, to change the minds of other Republican Jewish community leaders.

77. According to a February 13, 2018 article in *Tablet Magazine*, "Muzin largely failed to persuade Jewish leaders to agree to meetings with influential Qataris visiting New York for the opening of the United Nations General Assembly." By and large, American Jewish leaders declined to meet with the Emir of Qatar when he was at the United Nations in September of 2017 and declined offers of all-expenses-paid trips to visit Qatar.

C. Defendants Target Elliott Broidy.

78. Muzin admitted that he identified and described Mr. Broidy to the Qatari government as an impediment to Qatar's foreign policy interests in the United States. In connection with his work for Qatar, Muzin or his employees or agents participated in weekly meetings at the Qatari Embassy in Washington, D.C., where they discussed the ongoing efforts against Mr. Broidy. Defendant Muzin specifically mentioned Mr. Broidy in these meetings as an obstacle that needed to be dealt with for his lobbying on behalf of Qatar to succeed.

79. Muzin knew an associate of Mr. Broidy, Joel Mowbray. Mowbray and Muzin were professional colleagues and friends. Mowbray introduced Muzin to Senator Cruz because Mowbray believed Muzin's support of Israel was the same as his. It is because of this prior relationship that Muzin met with Mowbray in late February and early March 2018—on at least three occasions—both before and shortly after the media started publishing stories on Mr. Broidy using the hacked emails as a source of information.

80. As Muzin admitted to Mowbray, "Broidy's name comes up in Embassy meetings often." Muzin also stated, "I definitely identified him as somebody who, was not, didn't like them too much." Muzin stated, "There's no question I had conversations with them [the Qataris] about Elliott [Broidy]." Muzin also admitted, speaking of his Qatari clients, "They knew about him [Broidy]" and "knew that he [Broidy] had been influential" in shaping the White House's views on Qatar."

81. [redacted]

82. [redacted]

83. [redacted]

84. [redacted]

[redacted]

85. Benomar was also in close contact with Muzin and Allaham and worked with them to target Broidy. Allaham and Benomar had approximately fifty phone calls between June and November 2017 and, on August 6, 2017, Muzin established a group chat for the three of them on the text message service WhatsApp, which they used to communicate regarding their business.

86. [redacted] after Howard's then-employer, Conover, had declared on its FARA disclosures that he and the firm had ceased working for Qatar, but while the hacking against Broidy's computer systems was ongoing and throughout the media dissemination phase of the conspiracy.

87. The criminal enterprise targeted Mr. Broidy specifically because he had exercised his right to speak out on an issue of national and international concern and by doing so, had frustrated Qatar's interests.

IV. The Qatari Enterprise Executes an Unlawful Scheme to Hack Plaintiffs' Computer Systems.

88. As part of its efforts to discredit Broidy, the Qatari Enterprise, based, in part, on the efforts of Defendants, agreed to engage in, and did in fact coordinate, a series of cyberattacks and other misappropriation of Broidy's private communications and documents. Each Defendant acted in furtherance of the goal of the conspiracy and criminal enterprise, as alleged below.

89. On information and belief, sometime prior to December 27, 2017, the Qatari Enterprise retained Global Risk Advisors ("GRA"), an international strategic consultancy and cyber security firm based in New York City, to coordinate an offensive cyber and information operation against Plaintiffs, including by infiltrating Plaintiffs' computer networks and obtaining unauthorized access to Google email accounts of United States persons associated with Plaintiffs.

90. Approximately two months before the cyberattacks against Plaintiffs and their associates began, in October 2017 GRA opened a subsidiary of GRA organized under the laws of Gibraltar and physically located in Doha, Qatar.

91. On information and belief, David Mark Powell is a former British intelligence operative who established GRA's office in Qatar and runs GRA operations from that office.

92. On information and belief, GRA was actively recruiting new employees within the small community of former U.S. government offensive cyber operatives, and GRA made it clear within that community that they had been retained to conduct or coordinate offensive cyber operations on behalf of Qatar.

93. On information and belief, GRA employees Kevin Chalker and David Mark Powell had knowledge of Qatar's hacking scheme and intentionally furthered the scheme by hiring cyber operatives and personally supervising the hackings into Plaintiffs' email servers and computer systems.

94. On information and belief, GRA introduced Qatar to cyber mercenaries in various countries to coordinate technical aspects of the illegal intrusion into Plaintiffs' email server and Google LLC's servers, and the dissemination of the contents to U.S. news organizations, including individuals or groups associated with known mercenary cyber threat actors.

95. On information and belief, the individuals and entities identified by GRA and used by the criminal enterprise to attack Plaintiffs included: Omniscope Limited, a U.K. security and intelligence firm; a naturalized Israeli citizen with a history of criminal activity; and a London-based strategic intelligence firm with offices in the United States.

A. Hackers Target Robin Rosenzweig with Spear Phishing Emails.

96. Robin Rosenzweig, a U.S. citizen and Mr. Broidy's spouse, serves as legal counsel to Plaintiffs and lives in Los Angeles. Ms. Rosenzweig has an email account through Gmail, an email service provided by Google LLC ("Google")—a company headquartered in Mountain View, California. Ms. Rosenzweig's Gmail account contains private communications and requires at least a username and password for access.

97. On December 27, 2017, Ms. Rosenzweig received an email at her Gmail account that appeared to be a security alert from Google. The email used Google trademarks without the permission of Google, including the Google logo and the Gmail logo. It was sent from a Gmail address and had been disguised to look like an authentic security alert from Google. The email purported to alert Ms. Rosenzweig that the security on her account had been compromised and that she needed to verify or change her account credentials.

98. When she clicked on the link in the email, it directed her to a TinyURL website that appeared as if it was an authentic Google account login page. TinyURL is a redirecting service that provides shortened URLs that redirects a website visitor to the website associated with the longer, masked URL. It is known to be used by hackers and scammers to avoid detection and circumvent spam and malware filters. The URL address for that page was http://tinyurl.com/yaw4jmpn. When the TinyURL link was clicked it redirected Ms. Rosenzweig to a website that contained Google's logo and appeared to be an authentic Google account update page. However, that page was a fraudulent login page that is no longer active. The TinyURL

link has since been terminated by TinyURL for being used for spam, fraud, malware, or other illegal activity.

99. That email was a fraudulent "spear phishing" email. Spear phishing is the use of a fraudulent electronic communication targeted towards a specific individual, organization or business in order to steal data or install malware on a targeted user's computer. This spear phishing email was designed to gain unauthorized access to Ms. Rosenzweig's Google accounts, which include the full suite of Google's online products, such as Gmail, Google Drive, Google Calendar, Google Contacts, and YouTube. Those accounts contained, among other things, personal emails, business emails, usernames and passwords to access other non-Google accounts, including an account on the computer network of Plaintiff BCM. Without authorization and in violation of Google's Terms of Service, the cyberattackers used Ms. Rosenzweig's credentials to unlawfully access passwords stored by Ms. Rosenzweig on Google's servers. Gmail Program Policies and Google's Terms of Service expressly prohibit illegal uses as well as sending unauthorized email of any person without their consent.

100. Ms. Rosenzweig's Gmail account was accessed and modified unlawfully and without her consent on or around January 3, 2018, by hackers using the "Mail.ru" service. The attackers modified Ms. Rosenzweig's email account settings so that emails containing "Mail.ru," "viewed," or "alert" were marked as read and moved immediately to her trash folder. The attackers did this to ensure that any legitimate security alerts would not be viewed by Ms. Rosenzweig. "Mail.ru" signifies a Russian email service that publishes an app that can be used to send and receive emails on Mail.ru or other email services like Gmail. Unbeknownst to Ms. Rosenzweig, on January 4, 2018, Ms. Rosenzweig received a true security alert—that went directly to her trash folder—notifying her that a user or users of the Mail.ru app had obtained

access to read, send, delete, and manage her Gmail account, all without her awareness or consent. The hackers thereby gained control of Ms. Rosenzweig's Gmail account through Mail.ru.

B. Hackers Target Elliott Broidy's Executive Assistant with Spear Phishing Emails.

101. Elliott Broidy's Executive Assistant is a U.S. citizen and resident of Los Angeles, CA. She is an employee of Plaintiff BCM. The Executive Assistant has a private Gmail account, which is used to send and receive personal emails, including private communications and requires at least a username and password for access.

102. On or around January 14, 2018, just weeks after Ms. Rosenzweig was attacked, the Executive Assistant began to receive spear phishing emails disguised as Google security alerts, which bore Google trademarks used without Google's permission and were sent through Google's Gmail service in violation of Google's Terms of Service and Gmail's Program Policies.

103. One of the fake spear phishing emails contained a fictitious security alert with a picture of the Executive Assistant's face and part of the Executive Assistant's phone number. The email was sent from a misleading Gmail account with the name "Gmail Account" and the email address noreply.user.secure.services@gmail.com, which had been drafted to look like an authentic security alert from Google. The email purported to alert the Executive Assistant that the security on the account had been compromised and that the Executive Assistant needed to verify or change the Google credentials.

104. When the Executive Assistant clicked on the link in the email, it directed the Executive Assistant to an Owly address, which redirected to a website that appeared as if it were an authentic Google account login page.

105. Like TinyURL and Bitly, Owly is a redirecting service that provides shortened URLs that redirect a website visitor to the website associated with the longer URL. It is known to be used by hackers and scammers to avoid detection and circumvent spam and malware filters. When the Owly link was clicked, it redirected the Executive Assistant to the following website that contains Google's logo and appeared to be an authentic Google account login page: http://loms.96.lt/BDHRov58?platform=hootsuite. However, that page was a fake login page that is no longer active.

106. On or about December 27, hackers used similar spear phishing methods in an unsuccessful attempt to unlawfully access Mowbray's Google email account.

C. Hackers Infiltrate BCM's Servers.

107. Plaintiff BCM has an exchange server physically located in Los Angeles, California, that allows BCM employees to send and receive business and occasional personal emails. Mr. Broidy, his Executive Assistant, and several other employees all have secure email accounts on the BCM server containing private communications that require at least a username and password for access.

108. Efforts to gain unlawful access to Plaintiff BCM's network in California appear to have commenced as early as January 7, 2018. The first successful access was gained on January 16, 2018, just two days after the successful spear phishing campaign on Mr. Broidy's Executive Assistant.

109. The attackers maintained unauthorized and unlawful access to the BCM email server until at least February 25, 2018. During this period, there were thousands of instances of unlawful and unauthorized access to corporate email accounts at Plaintiff BCM, including but not limited to unlawful and unauthorized connections to Mr. Broidy and his Executive

Assistant's email accounts at Plaintiff BCM. Each of these intrusions required the use of stolen or altered credentials.

110. The exploitation of BCM's mail server was enabled by thousands of Virtual Private Network ("VPN") connections that obfuscated the origin of the attack.

111. VPNs route internet communication through additional networks to hide the original source of the connection. Some of these VPN connections occurred via IP addresses that are allocated to United States companies that lease them to third parties. For example, one of the suspicious IP addresses associated with the intrusions into the BCM server was leased from Micfo LLC, a company headquartered in Charleston, South Carolina.

112. Plaintiffs retained Ankura Consulting LLC ("Ankura") on March 2, 2018, to investigate the compromise of Ms. Rosenzweig's Gmail account. Their investigation detected evidence of unauthorized access. While much of the artifacts discovered during the investigation included the hackers using VPN technology, Ankura's investigation also discovered non-VPN connections from Qatar and Vermont.

113. Ankura's review of mail server artifacts uncovered that on February 14, 2018 and February 19, 2018, two unlawful and unauthorized connections into BCM's California server originated from an IP address in Qatar. These two unlawful and unauthorized intrusions were not masked by VPNs—even though the connections immediately before and immediately after the access were routed through VPNs—possibly because the VPN failed or because the accessing computer automatically connected to Plaintiff BCM's network before the VPN could be activated. These connections represent suspected unmasked intrusion signals accessing BCM's network from an IP address in Qatar.

114. Additional non-VPN masked connections occurred between February 12 and February 25 of 2018. During that period, hackers utilizing two separate Vermont IP addresses directly accessed Plaintiffs' servers at least 178 times.

115. Based on Ankura's forensic investigation, the spear phishing emails and hacking intrusions used wires to transmit signals across state lines. Ankura documented unauthorized access from U.S-based VPN servers as well as VPN servers overseas that were previously reported to be favored by criminal actors.

116. From January 16, 2018 to February 25, 2018, hackers accessed Broidy's and BCM's mail server, which is known to contain emails, attorney-client privileged information, private communications, corporate and personal documents, copyrighted material, and contracts, business plans, confidential and sensitive proprietary information, and trade secrets and other intellectual property.

117. These attacks resemble a pattern of known international attacks by sophisticated cyber-hackers. Previous attacks against other victims by these same threat actors have involved similar fake news alerts, malicious Google login pages, email addresses designed to resemble legitimate Google security addresses, falsified two-factor authentication messages, and the use of Mail.ru to control victims' accounts.

118. Mr. Broidy was not the only outspoken critic of Qatar targeted by the hacking scheme. More than one thousand individuals have been victimized by similar hacking intrusions by the Qatari Enterprise since at least 2014.[1] The victims range from high-profile figures in

[1] *See* Shmuley Boteach, "Qatar's War to Destroy Pro-Israel Jews," *Jerusalem Post*, Oct. 8, 2018, https://www.jpost.com/Opinion/Qatars-war-to-destroy-pro-Israel-Jews-568942; Eli Lake, "Russian Hackers Aren't the Only Ones to Worry About," *Bloomberg*, Sept 18, 2018, https://www.bloomberg.com/opinion/articles/2018-09-18/russian-hackers-aren-t-the-only-ones-to-worry-about.

government, business, journalism, and human rights advocacy in the United States, Europe, the Middle East and elsewhere around the world. Dozens of United States citizens and organizations have been targeted and injured, including former intelligence officials, former staffers from the Democratic National Committee and the Hilary Clinton Presidential campaign, high-profile political activists opposed to the Assad regime in Syria, and a researcher at a Washington, D.C., think tank currently investigating foreign influence in the 2016 elections. Other targets include FIFA soccer stars, former European defense officials, South Indian film actors and actresses, and hundreds of government leaders and diplomats across the Middle East. The hacking conspiracy also targeted users of "@un.org" email addresses, journalists, and lobbyists.

119. In particular, one other prominent critic of Qatar targeted by the hacking conspiracy was American Rabbi Shmuley Boteach. Upon information and belief, another target was a close associate of President Trump in the White House.

120. These numerous attacks have extended over years and represent a pattern of unlawfully accessing victims' computer systems to extract private information, extortion material, or other items of value.

V. The Criminal Enterprise Uses Stolen Documents to Injure Broidy.

121. Allaham wrote to Muzin on WhatsApp on March 13, 2018, that Benomar had gone to Qatar prior to the date of the message "to get the emails. That what [*sic*] I think he was doing there [in Qatar]." Muzin responded by referencing Mr. Broidy by name.

122. After unlawfully obtaining Plaintiffs' private communications, emails, documents, and intellectual property, hackers and/or their co-conspirators within the United States converted the stolen materials to PDF files and physical printouts for dissemination to third parties, including journalists. Many of the PDFs disseminated to third parties contain time

stamps different from the Pacific Time Zone associated with the original documents—and instead bear time stamps from the Central and Eastern Time Zones.

123. On February 24, 2018, members of the Qatari Enterprise registered the email address "LA.Confidential@mail.com" through the company 1&1 Internet, Inc., which operates in the United States through offices in Chesterbrook, Pennsylvania. Mail.com provides free email addresses akin to Google's Gmail service.

124. Plaintiffs' stolen emails have also appeared on a website hosted by a United States company, GoDaddy LLC ("GoDaddy"), which is headquartered in Scottsdale, Arizona. GoDaddy is a domain registrar and web hosting service that sells website domains to users so they may create their own webpage and host websites. The hackers further obfuscated their identity using a registration masking service, Domain by Proxy LLC, which allows a user to replace their own personal information with information belonging to Domain by Proxy LLC for purposes of registration. Domain by Proxy LLC is a company owned by GoDaddy LLC.

A. Defendants Coordinate a Smear Campaign Against Broidy Using Hacked Documents.

1. Defendant Howard Places Media Stories Using the Hacked Documents.

125. During the relevant time period, Defendant Gregory Howard had extensive contacts with both members of the Qatari Enterprise and reporters working on stories about Mr. Broidy that were based on the materials stolen from Plaintiffs' computer systems and servers. The volume and timing of these contacts show that Howard was acting in concert with Defendants and the Qatari Enterprise during this period.

126. Howard's phone records show that he orchestrated a sophisticated media and distribution campaign, [redacted], to place information

illegally obtained from the hacking in the hands of journalists, media organizations, and public relations professionals.

127. [redacted]

128. Howard's phone calls following the hacking showed that he was in close and frequent communication with journalists in the early months of 2018 before they began publishing stories that relied on information stolen from Plaintiffs' computer systems and servers. In some instances, Howard communicated with journalists weeks before they published these articles. The intensity of those contacts often increased in the days prior to publication. During this same period, Howard closely communicated with public relations experts, research groups, and registered agents of Qatar to coordinate the media disinformation campaign against Broidy.

129. Starting on January 7, 2018, three days after the first successful spear phishing intrusion, Howard engaged in a flurry of calls with outside public relations professionals, his then-colleagues at Conover & Gould, and Diogenes Group Research ("Diogenes"), a Florida-based research and graphic design company.

130. From January 18, 2018, through May 22, 2018, Howard participated in more than two hundred phone calls with reporters who contributed to stories regarding Broidy and Qatar or regularly covered Qatari-related issues. These included extensive, and at times, almost daily calls with now-former AP reporter Tom LoBianco, all before the time he authored several stories regarding Mr. Broidy in March and May 2018 based on the contents of his hacked email. In addition, Howard conducted more than a dozen calls with the *New York Times*, *McClatchy*, the

Wall Street Journal, and the *Washington Post*, all of which were focusing on stories regarding Broidy's hacked emails.

131. On February 21, 2018, Howard engaged in a call lasting over 40 minutes with a reporter in the Washington, D.C. office of the *New York Times*. Later that day, Howard received a call from an unknown individual located in the *New York Times* Washington bureau. Just under two hours later, Howard called the direct dial office phone number of the *New York Times*' lead investigative reporter, Mark Mazzetti.

132. At the time, the *New York Times* was researching the story about Mr. Broidy and George Nader that would be published on March 3, 2018. Mazzetti was the lead author of the piece. This story relied significantly on Plaintiffs' documents unlawfully obtained through hacking.

133. In the late morning on March 2, 2018, in the early stages of media inquiries based on the hacked emails and the day before the first such story in the *New York Times*, Howard [redacted]. Then, less than an hour later, Howard exchanged two calls with Diogenes, the second of which lasted over 9 minutes. Howard [redacted] and later had a call lasting over 15 minutes with a reporter at the Washington, D.C. office of the *New York Times*.

134. On March 23, 2018—three days before the AP published an article based on Mr. Broidy's emails—LoBianco, one of the authors of the piece, called Howard three times in less than an hour, with these calls lasting nearly 40 minutes total. Less than thirty minutes after that final call ended between LoBianco and Howard, LoBianco emailed the first and only batch of hacked emails that his outlet provided to Mr. Broidy's associates before AP published its March 26 article.

135. In the two weeks prior to the release of this article, Howard had multiple phone calls every day with LoBianco, the duration totaling almost seven hours. Before March 12, 2018, Howard's phone records show no contacts with LoBianco. Over the next two months, however, Howard continued to be in extensive, and at times, almost daily contact with LoBianco, as LoBianco continued to pursue stories based on Broidy's stolen emails.

136. On March 24, 2018, LoBianco and Howard had at least two conversations, lasting a total of over 30 minutes, and they exchanged two more calls the next day, March 25. Minutes after the second call between Howard and LoBianco on that day, which lasted over 18 minutes,

[redacted]

137. On March 26, 2018, the Associated Press ("AP") published an article by LoBianco and other staff, based on documents stolen from the cyberattack. The article noted that "[s]cores of Broidy's emails and documents have leaked to news organizations," but did not indicate that the stolen materials were provided by an "anonymous" source.

138. On March 28, 2018, Howard spoke for more than 20 minutes with *New York Times* reporter Ken Vogel. The next day, Vogel retweeted a since-corrected *Newsweek* story, and made disparaging remarks about Mr. Broidy. Vogel later deleted the tweet.

139. On April 27, 2018, LoBianco notified an associate of Mr. Broidy, "We got a new batch of emails." In the days leading up to that message, LoBianco and Howard exchanged at least four phone calls between April 18 and April 24, which totaled approximately 45 minutes. On May 2, 2018, Howard called LoBianco at least once early that evening.

140. On May 8, 2018, Howard and LoBianco exchanged calls, with at least one call lasting more than nine minutes, followed by at least one call between the pair on each of the next two days.

141. On May 11, 2018, LoBianco emailed to Mr. Broidy's representatives a first batch of images of Broidy's hacked emails upon which he planned to report for what became his second article in the AP based on Mr. Broidy's emails. That article was published on May 21, 2018.

142. On May 11, 2018, Howard and LoBianco had at least two conversations that afternoon, hours before LoBianco sent to Mr. Broidy's representatives copies of the hacked emails.

143. The final batch of hacked emails that LoBianco provided to Mr. Broidy's representatives was sent on May 18, 2018.

144. In total, between March 12 and May 22, 2018, Howard and LoBianco logged nearly fifteen hours of time over the phone. During the entire time Howard was in conversations with LoBianco, Howard was not registered as a foreign agent representing the Qatari interests.

145. In Conover & Gould's FARA Supplemental Statement filed on February 28, 2018, the firm claimed that it terminated its work on behalf of Qatar on January 18, 2018—two days after the first successful breach of BCM's computer systems and servers. According to that Supplemental Statement, the last communication Howard had with a media entity on behalf of Qatar occurred on December 15, 2017, almost a month before the supposed termination date of Conover & Gould's representation of Qatar.

146. Howard did not register again as a foreign agent of any country until May 10, 2018, when he worked at his current firm, Mercury. According to Mercury's September 7, 2017 contract-modification FARA filing, Mercury's work on behalf of Qatar was focused on media relations; its monthly pay from Qatar increased to $120,000 that year; and its work would be overseen by the "Government Communications Office of the State of Qatar."

147. Before assuming his role at his current firm Mercury on May 10, 2018, Howard had approximately two dozen calls with members of the firm, almost all of which came at key times in the planning or execution of the media dissemination phase of the conspiracy. Several of the phone lines he contacted are registered to registered Qatari agents Katherine Lewis and Jennifer Kaufmann, as well as Molly Toomey, whose bio on the Mercury website states that she "[l]ed international PR" for a "$1 billion" project financed by Qatar Investment Authority.

148. Although Mercury has acted for years as a FARA-registered agent of Qatar, Howard's Short Form registration submitted in May 2018 as an employee of Mercury omitted Qatar as one of the foreign principal clients whose interests he was registering to represent. Mercury's FARA filings indicate that Howard's first foreign principal-related media interaction happened on May 22, precisely one day after the May 21 publication of LoBianco's second and final AP story on Mr. Broidy.

2. Defendants Muzin and Allaham Celebrate Their Conspiracy and Share Advance Notice of Media Accounts of Plaintiffs Based on the Hacked Emails.

149. Muzin and Allaham's text messages demonstrate Muzin's and Allaham's direct and prior knowledge of the hacking and their knowing use of stolen documents.

150. During the time of the cyberattacks against Broidy, Muzin was in Qatar.

151. On January 25, 2018, shortly after the successful hacking of BCM began, Muzin sent Allaham a message on WhatsApp, stating, "It's very good. . . . We got the press going after Broidy. I emailed you." Muzin and Allaham shared stolen information gained from the cyberattack with journalists in order to convince them to "go[] after Broidy."

152. On January 25, 2018, prior to the first public reports in the United States of materials stolen from Plaintiffs, Ben Wieder, a reporter for *McClatchy*, a Washington, D.C.,

publication focused on politics, emailed Defendant Muzin to tell him, "I'm working on a story about Elliott Broidy and was hoping to talk." Muzin, who at the time was still in Qatar after having flown there within a few days of the hackers' first successful breach into the BCM servers and computer systems, forwarded this message to Allaham and commented, "Time to rock." Less than an hour after sending the email to Muzin, Wieder called Howard, and they spoke for more than 10 minutes. Wieder would go on to write extensively about Mr. Broidy on the basis of carefully curated emails and other documents stolen from Broidy's servers.

153. On March 1, 2018, the contents of emails stolen from Plaintiffs' computer accounts and servers appeared for the first time in media accounts, in a *Wall Street Journal* article that noted that it was based on "a cache of emails from Mr. Broidy's and his wife's email accounts that were provided to the Journal."

154. Muzin shared the *Wall Street Journal* article with Allaham over WhatsApp that same day. Muzin then commented, "He's finished."

155. Additional emails stolen from BCM's accounts and servers were published or reported on in other media outlets including the *Huffington Post* on March 2, 2018, which reported based on "[e]mails and documents an anonymous group leaked to HuffPost," as well as the BBC on March 5, 2018.

156. Muzin admitted to having foreknowledge of impending media stories about Mr. Broidy based upon the hacked material. On February 28, 2018, Defendant Muzin called Joel Mowbray and informed him that the *Times* was about to publish a story about Mr. Broidy and George Nader, saying that he received this information from his "media guy." [redacted]

157. On March 3, 2018, approximately two hours before the online publication of the *New York Times* story, [redacted] Upon information and belief, Defendant Muzin's "media guy" is Howard.

158. On WhatsApp, Allaham shared a link to the March 3, 2018, *New York Times* story about Nader with Benomar. On March 5 and 6, Allaham shared other articles about the hacking with Benomar.

159. On March 13, 2018, Muzin remarked to Allaham via WhatsApp that recent news stories about Broidy have "[p]ut[] him in [M]ueller['s] crosshairs." This communication demonstrates one of the central goals of the Qatari Enterprise—to portray Mr. Broidy as a target of special counsel Robert Mueller's investigation. Muzin's WhatsApp message to Allaham was sent less than an hour after [redacted]

160. On March 26, 2018, *McClatchy* published a story that discussed Mr. Broidy, authored by Ben Wieder. It was only one of a series of articles hostile to Mr. Broidy authored by Wieder following contact with Muzin and Howard, who also had extensive communications with Wieder's editor Viveca Novak and his frequent writing collaborator, Peter Stone.

161. On March 14, 2018, Muzin told Allaham on WhatsApp that he'd "get some intel about the Broidy event soon." This comment likely refers to a March 13, 2018, Republican fundraiser headlined by the President of the United States, for which Mr. Broidy had been listed as an event host.

162. The next day, on March 15, 2018, Muzin exclaimed to Allaham, via WhatsApp, "Elliott Broidy was not at the fundraiser!" Muzin and Allaham were excited at the prospect of furthering their objective of politically damaging Mr. Broidy.

163. Ten days later, on March 25, 2018, a front-page story in the *New York Times* reported extensively on Mr. Broidy's fundraising and business activities. The story reported that Mr. Broidy had agreed not to attend the March 13 fundraiser. The story was based, in part, on "[h]undreds of pages of Mr. Broidy's emails, proposals and contracts" received from what the *Times* euphemistically termed "an anonymous group critical of Mr. Broidy's advocacy of American foreign policies in the Middle East." This "anonymous group" is the Qatari Enterprise.

164. On March 21, 2018, the *New York Times* published a front-page article noting that an "anonymous group critical of Broidy's advocacy of American foreign policies in the Middle East" has been distributing "documents, which included emails, business proposals and contracts," belonging to Plaintiffs. On March 23, 2018, *Bloomberg* published an article about Mr. Broidy, which noted that it had "received two separate documents this week purporting to be versions" of materials belonging to Mr. Broidy.

165. Based on phone and text records, Benomar also played a role in placing information obtained from the hack in the hands of journalists and media groups. In this effort he worked closely with James Courtovich of Sphere Consulting, who is a registered agent of Qatar. Benomar and Courtovich conducted more than a dozen known calls and text messages between February and April of 2018, including several texts on April 13.

166. The following day, April 14, 2018, Courtovich met with Julie Bykowicz of the *Wall Street Journal*, according to his FARA Supplemental Statement filed on October 30, 2018. On April 18, 2018, the *Wall Street Journal*'s Bradley Hope, a colleague and frequent collaborator of Bykowicz, reached out to Mr. Broidy's representatives with a lengthy set of

questions relating to a new, previously unreleased batch of hacked emails. The *Wall Street Journal* ultimately did not publish the story.

167. On May 1, 2018, Courtovich emailed the *Wall Street Journal*'s Rebecca Ballhaus, according to his FARA filing. The next day, on May 2, Ballhaus contacted Broidy's representatives asking questions for an intended "profile," which would be substantially based on the contents of Mr. Broidy's hacked emails. The *Wall Street Journal* ultimately did not publish the story.

168. On May 4, 2018, Muzin contacted Allaham via WhatsApp. Muzin told Allaham that "our new friends can make Broidy go away altogether."

169. On October 26, 2018, Stonington filed a FARA supplemental statement indicating that Muzin terminated his representation of Qatar "[n]o later than August 21, 2018." Muzin has failed to disclose any payment he received from Qatar after February 6, 2018, or payment for any activities described above.

170. Media outlets in the United States and abroad continue to publish—and to threaten to publish—materials stolen from Plaintiffs. Plaintiffs continue to receive numerous press inquiries concerning such materials.

171. All of this evidence, obtained through limited discovery to date, is highly probative of the fact that Muzin, Allaham, and Howard had received and were knowingly using the stolen emails. It is likely that after a reasonable opportunity for further investigation or discovery, Plaintiffs would produce additional evidentiary support to establish these allegations.

B. Qatar Pays Muzin and Allaham Millions of Dollars for their Role in the Scheme.

172. Defendants' involvement in this tortious scheme coincided with their receipt of millions of dollars of compensation from Qatar and Qatari interests.

173. [redacted]

174. [redacted], on September 18, 2017, and again on October 10, 2017, Muzin's firm received a total of $3.9 million, in two separate installments of $1.95 million each, from BlueFort Public Relations LLC ("BlueFort"). Muzin did not report this payment until the following year, on October 26, 2018. On that October 26 FARA disclosure, Muzin states that his firm was paid such an exorbitant sum because he "made senior level introductions, arranged trips, and fostered dialogue" on behalf of Qatar.

175. BlueFort is one of the outwardly legitimate faces of the Qatari Enterprise. It is a shell corporation with an office address listed in Doha, working to promote Qatari interests in the United States. But upon information and belief, and despite claims that it is a private company, BlueFort receives its funding from Qatar and is, for all practical purposes, an alter ego of Qatar. BlueFort serves as a front for the "black ops" team used by Qatar to mastermind Qatar's successful bid for the 2022 FIFA World Cup, a bid that has been shrouded in controversy and has led to a dozen criminal convictions and guilty pleas relating to corruption charges.[2]

176. BlueFort was a sham corporation. Media has reported that "Blue Fort appears to have acted as a conduit for lobbying payments."[3] Despite claiming a presence in the United

[2] *See* "Exclusive: Qatar sabotaged 2022 World Cup rivals with 'black ops,'" *The Sunday Times*, July 29, 2018, https://www.thetimes.co.uk/article/exclusive-qatar-sabotaged-2022-world-cup-rivals-with-black-ops-glwl3kxkk.

[3] *See* Dan Friedman, "Qatari Lobbyists Received Millions Through Shadow Firm," *Mother Jones*, Jan. 8, 2019, https://www.motherjones.com/politics/2019/01/qatari-lobbyists-received-millions-through-shadow-firm/.

States, United Kingdom, and Qatar, BlueFort does not appear in available corporate registries of either the U.S. or UK, does not appear to have its own office space in any of the countries in which it claims to operate (its Washington D.C. office appears to share a virtual office, and its London office is a Regus shared office space), and its website consists of a single, sparse page. This sole web page indicates that the company "Spark Digital" is an affiliate of BlueFort. Spark Digital's LinkedIn profile page describes itself as being "the team that brought you the Qatar 2022 World Cup bid website and social media campaign."

177. Muzin stated that of the $3.9 million he received from BlueFort, he paid $2.3 million to Joseph Allaham for "services rendered."

178. Muzin received a pay raise from Qatar that coincided with the timing of cyber and media operations against Mr. Broidy. Notwithstanding Muzin's lack of success with the Jewish community, Qatar raised his official, publicly disclosed pay to $300,000 a month, retroactively applied to the beginning of November 2017, but the decision to do so happened only days before Plaintiffs were victimized by an extensive cyberattack, as described above.

179. Defendant Allaham has at present still not reported, as required by FARA, the work he performed for BlueFort or the payment he received.

180. According to Muzin's FARA filings, on December 15, 2017, twelve days before the start of the first hack attempts, he received a $500,000 balloon payment from Qatar. This represented the raise of his regular monthly payments from Qatar from $50,000 a month to $300,000 month for both November and December combined. [redacted]

[redacted]

181. According to available FARA filings, Muzin and Allaham have received a total of at least $7 million for their work on behalf of Qatar, including their payments from BlueFort.

182. Even in the world of highly-compensated lobbying and public relations professionals working on behalf of foreign powers, these amounts far exceed the prevailing market rates for lobbying or political action.

183. Based on these circumstances, including the closeness in time between these substantial payments and the hacking of Plaintiffs and dissemination of hacked emails to the media, it is reasonable to infer and conclude that Defendants were aware of the Qatari Enterprise's efforts to attack Plaintiffs and that these payments were compensation to Defendants for their role in the conspiracy and unlawful scheme.

VI. Defendant Muzin Admits His Role in the Qatari Enterprise and Attempts to Extort Broidy and Joel Mowbray.

184. Muzin admitted his own complicity in the Qatari Enterprise in a series of meetings between Muzin and Joel Mowbray, in which Muzin acknowledged that Qatar was targeting Mr. Broidy and attempted at various times alternatively to extort and bribe Mowbray into working for the criminal enterprise.

185. These three meetings occurred on (1) February 27, 2018 at the Four Seasons Hotel in Georgetown, Washington D.C.; (2) March 5, 2018 at the Marriott Marquis in Washington, D.C.; and (3) March 8, 2018, at the Willard Hotel in Washington D.C.

186. During the February 27 2018, meeting, Defendant Muzin at first attempted to recruit Mowbray to accomplish the Qatari Enterprise's goals and "play a constructive role in ending this blockade effectively." Mowbray declined the overture.

187. Defendant Muzin demonstrated foreknowledge of press reports about Mr. Broidy based on illegally obtained information when he informed Mowbray during the February 27, 2018 meeting that the "*New York Times* is digging about . . . a connection to George Nader" and would be researching issues relating to Mr. Broidy, the Middle East and George Nader. This was the first time that Mowbray had ever learned of the existence of George Nader, and it was prior to any contact from anyone at the *New York Times* to Mr. Broidy or any of his associates relating to its subsequent stories on his supposed relationship with Nader, based on the contents of hacked emails.

188. The first published report of any alleged connection between Nader and Mr. Broidy did not occur until, at the earliest, the evening of March 3, 2018, when the *New York Times* published an article, based on documents obtained through the hack, alleging ties between Nader and Mr. Broidy. The *New York Times* did not reach out to Mr. Broidy or any of his representatives relating to Nader or the hacked emails until March 1, 2018, or in other words after Muzin revealed to Mowbray his insider knowledge of the publication's work on a story primarily based on Mr. Broidy's hacked emails.

189. It is implausible that Muzin would have been in a position to know about the particular issues relating to Mr. Broidy, the Middle East and Nader that were about to become the focus of media attention, unless he had access to, and knowledge of, information illegally obtained from the hacking that had been provided to journalists working on the report.

190. During the March 5, 2018, meeting, Defendant Muzin stated that "I did not cause the Broidy stuff, just because I have information" and "I don't know all the details" about the Broidy hack. Based on his acknowledgment that he had "information" about the hacking, it is

reasonable to conclude that Muzin possessed substantial knowledge regarding the attack on Broidy that could be revealed through discovery.

191. Muzin informed Mowbray that there was "a lot more coming" from the *New York Times* and that Mr. Broidy was "in deep shit." Muzin further stated that "there may be hacking stuff in there," which Mowbray understood meant that the *New York Times* and other journalists would be using information illegally obtained from the hack to attack Mr. Broidy. Through this conversation Muzin demonstrated that he had advance knowledge of the cyberattack and the documents illegally obtained from it.

192. Muzin further acknowledged in this meeting that "it's possible" that Qatar had hacked his own phone and email accounts, and in fact that "it's possible they try to hack people." Mowbray interpreted Muzin's statement as acknowledging that Mowbray's concerns about Qatar's illegal activity were justified while still trying to preserve plausible deniability for what he knew about Qatar's hacking activity against Plaintiffs.

193. Muzin attempted to rationalize his work for Qatar, stating, "Whatever, I mean I took a chance on a controversial client." Again, Muzin could not with a straight face deny Qatar's involvement with illegal hacking schemes to his former friend and colleague.

194. Muzin attempted to change the subject from Qatar's illegal activity by offering to pay Mowbray for enlisting in the Qatari Enterprise, stating, "Well, let's make some money together." Mowbray again rejected the offer to be paid by Muzin to betray Mr. Broidy and aid the criminal enterprise.

195. When enlisting Mowbray did not work, Muzin attempted to threaten him regarding his association with Mr. Broidy: "Honestly, you should be a little bit concerned about

this. . . . You should (have a lawyer) because you're very well-known and influential" as someone with an "anti-Qatar" position.

196. In the third and final meeting between Muzin and Mowbray, on March 8, 2018, Defendant Muzin discussed meetings he had with his client Qatar while serving as a registered agent of Qatar. During those meetings, held at the Qatari Embassy, multiple operatives in Qatar's employ would share information, including about Mr. Broidy.

197. In this conversation, Muzin again resorted to extortion and threats. Muzin admitted to Mowbray that "Broidy's name comes up in Embassy meetings often" and "I definitely identified him as somebody who . . . didn't like them too much." Muzin further acknowledged that everyone he "fingered" was "in danger." He admitted that Qatar had assembled an enemies list of people who were considered "hurdles" to Qatar's interests. He warned Mowbray that Mowbray and Broidy needed "to be very careful," that Qatar is "going after you," and that "Honestly, I know they're after you and Broidy."

198. After making these threats, Muzin asked Mowbray, "[I]f you get a subpoena is Broidy going to pay for your lawyers?" Muzin stated that Mowbray "could be in a multi-million dollar hole" trying to fight public relations and legal campaigns against him on behalf of the Qatari Enterprise.

199. Mowbray understood that Muzin's purpose in talking to Mowbray was to use alternating offers of bribes and ominous threats to extort him into working for the Qatari Enterprise.

200. When Mowbray directly challenged Muzin regarding his knowledge of information that could be known only through access to the illegally obtained emails, Muzin at first stated that he got his information from the "Dark Web." When Mowbray told Muzin that he

suspected Muzin had helped initiate the cyber operation against Mr. Broidy, Muzin stated, "I was doing my job." Muzin then stated that he realized that he needed "to be a little more careful" when he spoke to Mowbray. When Mowbray asserted that Muzin was "neck deep in this conspiracy" against Mr. Broidy, Muzin replied, "I know."

VII. Plaintiffs Bring Lawsuits Against Individual Members of the Qatari Enterprise.

201. On March 19, 2018, Mr. Broidy and BCM, through counsel, formally requested that Qatar take appropriate action to halt the attacks on Plaintiffs' emails, documents, and data, to stop Defendants from disseminating Plaintiffs' emails, documents, and data, and/or to assist Plaintiffs in halting dissemination if the hack had been conducted by a rogue agent of Qatar.

202. When Qatar failed to respond to Plaintiffs' request, Mr. Broidy and Broidy Capital Management LLC filed suit in the United States District Court for the Central District of California against Defendant Muzin, Qatar, and several other individuals responsible for the hacking scheme on March 26, 2018. On May 4, 2018, the parties stipulated to a stay to permit limited jurisdictional discovery. In conducting this limited jurisdictional discovery, Plaintiffs were able to uncover the phone records for some of the Defendants and others, as well as some WhatsApp chats among Muzin, Allaham, and other conspirators. Plaintiffs have used this narrow opportunity for discovery to amply substantiate the above allegations. However, this discovery was limited to establishing jurisdiction in that case, and did not reach the merits of any of Plaintiffs' claims. The district court dismissed the lawsuit against Qatar on grounds of foreign sovereign immunity, and dismissed all other served defendants for lack of personal jurisdiction. The court did not reach the merits of any of Plaintiffs' claims, and its decision is currently under appeal.

203. On November 30, 2018, Plaintiffs also filed suit in the United States District Court for the Southern District of New York against Jamal Benomar. The district court

dismissed the case without permitting any jurisdictional discovery, on grounds of diplomatic immunity. The district court did not reach the merits of any of Plaintiffs' claims.

204. The Defendants named here enjoy no sovereign or diplomatic immunity, and therefore this Court may exercise jurisdiction over this suit. Defendants are all American citizens residing in the United Sates. They are not Qatari nationals, officials, or instrumentalities. They aided Qatar only on a contractual basis and for financial and commercial gain. Therefore, this action may proceed to the merits, and Plaintiffs may obtain full relief as prescribed by law. It is likely that after a reasonable opportunity for further investigation or discovery, Plaintiffs would produce evidentiary support to prove all allegations herein at trial.

CAUSES OF ACTION

COUNT ONE (all Defendants)
Violations of RICO Act, 18 U.S.C. § 1962(c) and § 1964

205. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

206. The federal RICO statue provides, "It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c).

207. The RICO Act further provides that "Any person injured in his business or property by reason of a violation of section 1962 of this chapter may sue therefor in any appropriate United States district court and shall recover threefold the damages he sustains and the cost of the suit, including a reasonable attorney's fee . . . ." 18 U.S.C § 1964(c).

208. Plaintiffs are "persons" who may sue under Section 1964(c).

209. Defendants are all "persons" subject to the Act.

A. The Qatari Enterprise is a Separate and Distinct Entity.

210. The Qatari Enterprise is an enterprise under the RICO Act that is distinct from Defendants. It was an association of Qatari officials and hackers, lobbyists and others who worked in common cause to serve Qatar.

211. Through all times relevant to this Complaint, Defendants have associated themselves with the Qatari Enterprise in fact, although not as a legal entity. Defendants committed the above-described tortious and criminal actions as part of a common purpose to serve the enterprise. These actions were separate and distinct from any legitimate work they performed under contract for Qatar.

212. The Qatari Enterprise consisted of, at least and potentially others, Qatar and its government and agents, Nicolas Muzin, Joseph Allaham, Gregory Howard, Jamal Benomar, Kevin Chalker, David Mark Powell, Ahmed al-Rumaihi, Mohammed bin Hamad bin Khalifa Al Thani, and numerous known and unknown agents, including cyber hackers, public relations professionals, lobbyists, political actors, and others. The criminal enterprise encompassed or corrupted numerous seemingly legitimate institutions and enterprises that provided structure and organization for the enterprise, including but not limited to BlueFort Public Relations LLC, Stonington Strategies LLC, Global Risk Advisors LLC, the Qatari Investment Authority, and the Qatari government and Embassy. All of these individuals and entities conspired to harm Plaintiffs and did cause them harm through a long-standing pattern of racketeering activity.

213. The Qatari Enterprise engaged in tortious conduct that crossed state lines, spanning from Qatar to California and Washington D.C. Defendants used their interstate media placement and lobbying services to advance the enterprise.

214. Plaintiffs hereby allege and set forth the following predicate racketeering activities as defined under 18 U.S.C. § 1961.

B. First Set of Predicate Offenses: Wire Fraud, in violation of 18 U.S.C. § 1343

215. Federal law imposes criminal penalties on "[w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice." 18 U.S.C. § 1343.

216. Defendants intentionally conspired with others to commit numerous acts of wire fraud by obtaining the login credentials of BCM employees through a scheme or artifice—*i.e.*, fake spear phishing emails.

217. At least one such fraudulent email was sent to Robin Rosenzweig. She received an email at her Gmail account that appeared to be a security alert from Google. The email used Google trademarks without the permission of Google, including the Google logo and the Gmail logo. It was sent from a Gmail address and had been disguised to look like an authentic security alert from Google. The email purported to alert Ms. Rosenzweig that the security on her account had been compromised and that she needed to verify or change her account credentials.

218. Hackers working with the Qatari Enterprise used similar spear phishing methods in an unsuccessful attempt to unlawfully access Mowbray's Google email account.

219. Another such fraudulent spear phishing email was sent to Mr. Broidy's Executive Assistant. These emails were disguised as Google security alerts, which bore Google trademarks used without Google's permission and were sent through Google's Gmail service in violation of Google's Terms of Service and Gmail's Program Policies.

220. One of the fraudulent spear phishing emails contained a fictitious security alert with a picture of the Executive Assistant's face and part of the Executive Assistant's phone

number. The email was sent from a misleading Gmail account with the name "Gmail Account" and the email address noreply.user.secure.services@gmail.com, which had been drafted to look like an authentic security alert from Google. The email purported to alert the Executive Assistant that the security on the account had been compromised and that the Executive Assistant needed to verify or change the Google credentials.

221. Defendants intentionally conspired with hackers who sent numerous spear phishing emails like the ones described above using interstate wires, and these transmissions crossed state lines.

222. Defendants intentionally conspired with hackers who used the spear phishing emails to make material misstatements that induced the targeted individuals to surrender their valuable login credentials.

223. Having fraudulently obtained those credentials through material misstatements, hackers acting on behalf of the Qatari Enterprise commenced an illegal cyberattack against Mr. Broidy and BCM's computer systems and servers. These cyber transmissions used interstate wires and crossed state lines—for example, forensic investigation has revealed that some transmissions traveled from Vermont to California. Defendants and their co-conspirators initiated thousands of intrusions into Plaintiffs' computer systems and email servers.

224. Defendants thereby obtained Plaintiffs' valuable electronic information, including but not limited to emails, private information, contracts, trade secrets, and business plans. Defendants launched the spear phishing attempts with the specific intent of fraudulently depriving Plaintiffs of their valuable property.

225. Defendants' tortious scheme targeting Broidy began in December 2017 and is ongoing.

226. Approximately 1,400 individuals have been victims of wire fraud through cyber hacking by the Qatari Enterprise, including dozens of American citizens.

227. As a direct consequence of Defendants' actions, Plaintiffs have suffered injury to their business or property, which include, but are not limited to, damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial.

C. Second Set of Predicate Offenses: Extortion in Violation of the Hobbs Act, 18 U.S.C. § 1951(a)

228. The Hobbs Act imposes criminal penalties on "[w]hoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do." 18 U.S.C. § 1951(a).

229. "'[E]xtortion' means the obtaining of property from another, with his consent, induced by wrongful use of actual or threatened force, violence, or fear . . . ." 18 U.S.C. § 1951(b)(2).

230. The law of the District of Columbia imposes criminal penalties on anyone who "obtains or attempts to obtain the property of another with the other's consent which was induced by wrongful use of actual or threatened force or violence or by wrongful threat of economic injury." D.C. Code § 22-3251(a). A violation of § 22-3251 is punishable by not more than ten years' imprisonment. § 22-3251(a).

231. On March 8, 2018, Defendant Muzin stated to Mowbray that "Broidy's name comes up in [Qatari] Embassy meetings often" and "I definitely identified him as somebody who . . . didn't like them too much." Muzin further acknowledged that everyone he "fingered" was "in danger." He further admitted that Qatar had assembled an enemies list of individuals who

were considered "hurdles" to Qatar's interests. He warned Mowbray that Mowbray and Mr. Broidy needed "to be very careful," that Qatar is "going after you," and that "Honestly, I know they're after you and Broidy."

232. After making these threats, Muzin asked Mowbray, "[I]f you get a subpoena is Broidy going to pay for your lawyers?" Muzin stated that Mowbray "could be in a multi-million dollar hole" trying to fight public relations and legal campaigns against him on behalf of the Qatari Enterprise.

233. Mowbray understood that Muzin's purpose in talking to Mowbray was to use threats of further illegal activity to obtain his intangible property—*i.e.*, Mowbray's services and cooperation with the Qatari Enterprise.

234. Muzin's threat caused Mowbray to reasonably fear that, if he did not cooperate with the Qatari Enterprise, he would be subject to further cyberattacks and publication of false and misleading information about him and Mr. Broidy that would cause severe economic damages and interfere in ongoing business dealings and relationships.

235. Mowbray's services regularly cross state lines. He regularly consults with clients in both Washington D.C. and California.

236. The Qatari Enterprise used its vast cyber hacking attack to threaten and silence Mr. Broidy, so that he would no longer criticize Qatar's sponsorship of terrorism.

237. This attempted extortion caused Plaintiffs substantial injury to their business and property and affected interstate commerce. Plaintiffs have had to expend considerable resources to defend themselves against further extortionate threats.

D. Third Set of Predicate Acts: Violation of the Travel Act (18 U.S.C. § 1952)

238. The federal Travel Act imposes penalties on "[w]hoever travels in interstate or foreign commerce or uses the mail or any facility in interstate or foreign commerce with the

intent to . . . promote, manage, establish, carry on, or facilitate the promotion, management establishment, or carrying on, of any unlawful activity" and "thereafter performs or attempts to perform" such an act. 18 U.S.C. § 1952(a).

239. "Unlawful activity" includes "extortion . . . in violation of the laws of the State in which committed or of the United States." 18 U.S.C. § 1952(b)

240. Muzin, a resident of Maryland, travelled to Washington D.C. with the intent of extorting Joel Mowbray and compel his cooperation with the Qatari Enterprise. Muzin then attempted, on three separate meetings with Mowbray in Washington D.C., to extort Mowbray with the threat of additional distribution of hacked information to journalists and media organizations.

241. This attempted extortion caused Plaintiffs substantial injury to their business and property and affected interstate commerce. Plaintiffs have had to expend considerable resources to defend themselves against further extortionate threats.

E. Fourth Set of RICO Offenses: Violations of the Defend Trade Secrets Act. 18 U.S.C. § 1832(a)(1) and (a)(5)

242. The Defend Trade Secrets Act imposes criminal penalties against anyone who "knowingly . . . with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information. . . ." 18 U.S.C. § 1832(a)(1).

243. The Defend Trade Secrets Act also imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). *See* 18 U.S.C. § 1832(a)(5).

244. Defendants and other members of the Qatari Enterprise repeatedly violated the Defend Trade Secrets Act, 18 U.S.C. § 1832, *et seq.* The BCM servers stored trade secrets including but not limited to highly confidential business plans and proposals, research supporting those plans and proposals including costs and service projections, information concerning business strategies and opportunities, and contacts for important business relationships.

245. These trade secrets are of substantial value to Plaintiffs, and they were used and intended for use in interstate and foreign commerce.

246. Plaintiffs take and have taken reasonable measures to keep this information secret. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

247. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

248. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

249. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

250. Defendants unlawfully conspired with persons who without authorization appropriated, obtained, and stole Plaintiffs' trade secrets. Those individuals knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs.

251. Defendants' knowing and intentional violation of the Defend Trade Secrets Act has materially injured Plaintiffs. It has deprived them of valuable trade secrets, and caused them to expend resources to defend against further cyberattacks.

252. The Qatari Enterprise's misappropriation of Plaintiffs' trade secrets began in January of 2018 and is ongoing.

253. As a direct consequence of Defendants' actions, Plaintiffs have suffered injury to their business or property, which include, but are not limited to, damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information; and harm to Plaintiffs' business, in an amount to be proven at trial.

F. Fifth Set of Predicate Acts: Economic Espionage, in Violation of 18 U.S.C. §§ 1831(a)(1) and (a)(5)

254. Federal law provides that "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret" violates 18 U.S.C. § 1831(a)(1).

255. Federal law also imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" a violation of § 1831(a)(1). *See* § 1831(a)(5).

256. Defendants unlawfully conspired with persons who without authorization took, appropriated, and obtained Plaintiffs' trade secrets through the cyberattack against BCM's servers. Defendants and other members of the Qatari Enterprise knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs. They misappropriated Plaintiffs' trade secrets intentionally for the benefit of their foreign client, Qatar, and acted with the knowledge that their actions would have the effect of benefiting the foreign government of Qatar.

257. Defendants unlawfully conspired with persons who used an artifice and fraud—the fake Gmail spear phishing emails—in order to take, appropriate, and obtain Plaintiffs' trade secrets.

258. Defendants unlawfully conspired with persons who used fake spear phishing emails to induce targets to surrender their valuable login credentials. Several targets did provide their login credentials in reliance of these false material statements.

259. As a direct consequence of Defendants' misappropriation, Plaintiffs have suffered injury to their business or property, which include, but are not limited to, damages resulting from harm to Plaintiffs' computers, servers, and accounts, loss in the value of Plaintiffs' trade secrets and business information, and harm to Plaintiffs' business, in an amount to be proven at trial.

G. Sixth Set of Predicate Acts: Criminal Copyright Infringement, in Violation of 17 U.S.C. § 506(a)(1)

260. Federal law provides that "[a]ny person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed . . . for purposes of commercial advantage or private financial gain." 17 U.S.C. § 506.

261. Plaintiffs' computer systems and email servers contained numerous copyrighted works protected under federal law.

262. Defendants unlawfully conspired with persons who hacked into Plaintiffs' computer systems and email servers. Defendants then violated Plaintiffs' copyright on those materials by indiscriminately copying them, and reproducing some of them in PDF form, and distributing them to media organizations and journalists.

263. The violation of Plaintiffs' copyright was intentional and willful.

264. Plaintiffs' copyrighted material was valuable, and Defendants illicitly obtained that value by stealing and reproducing Plaintiffs' copyrighted works.

265. Defendants violated Plaintiffs' copyright for purposes of commercial advantage or private financial gain. Defendants sought to harm Plaintiffs financially in order to silence Mr. Broidy, and thereby gain a commercial advantage in the form of eased sanctions. Moreover, Defendants were paid by the Qatari Enterprise to violate Plaintiffs' copyright.

266. As a direct consequence of Defendants' criminal copyright violations, Plaintiffs have suffered injury to their business and property, which include, but are not limited to, damages resulting from injury to Plaintiffs' value in their copyrighted information, in an amount to be proven at trial.

H. Pattern of Racketeering Activity

267. The Qatari Enterprise has engaged in a pattern of racketeering activity with relationship and continuity. More than one thousand individuals, many critics of Qatar and its allies, have been victimized by the criminal enterprise's cyberattacks and other racketeering activity since at least 2014. The enterprise committed these numerous incidents of racketeering activity for the purpose of silencing those critics. Thus, the Qatari Enterprise has committed a "closed-ended" scheme of racketeering violations.

268. Moreover, the Qatari Enterprise's campaign to silence its critics is ongoing, and it continues to commit acts of racketeering to shield Qatar from public scrutiny. Media organizations are still relying on information stolen from Mr. Broidy's computer systems and email servers to publish stories to damage his image. The enterprise has thus also engaged in an "open-ended" scheme of racketeering.

I. Defendants Exercised Management and Operation of the Enterprise.

269. Defendants operated and managed the affairs of the Qatari Enterprise and in particular implemented its media disinformation campaign against Plaintiffs. Muzin and Allaham were co-founders of Stonington Strategies, not mere employees; Howard has been a

manager at Conover and Mercury. Muzin "definitely identified" Mr. Broidy as a "hurdle" for the enterprise's goals of rehabilitating Qatar's diplomatic reputation, and thereby directed the attention and activities of the enterprise toward Mr. Broidy. Both [redacted] Howard acted in concert with Muzin and Allaham to manage and direct the placement of damaging stories about Mr. Broidy, derived from stolen and hacked information from Plaintiffs' servers, in the media. All Defendants exercised responsibility and management over the enterprise's affairs.

J. Effect on Interstate Commerce

270. The Qatari Enterprise has substantially affected interstate commerce by, for example, harming Plaintiffs' property and business, including but not limited to loss to and consumer goodwill and loss of valuable electronic information, business plans, contracts, trade secrets, copyrighted materials, and substantial expense in protecting Plaintiffs' computer systems and email servers from additional cyberattack.

K. Business Injury

271. As a direct consequence and by reason of Defendants' racketeering activity, Plaintiffs have suffered injury to their business and property, which includes, but is not limited to, financial damage resulting from loss of consumer goodwill and business relationships; damage to Plaintiffs' computers, servers, and accounts; loss caused by the investigation of the hackings and the securing of Plaintiffs' systems against further intrusions; and loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property, in an amount to be proven at trial. Plaintiffs are entitled to treble damages and attorneys' fees under 18 U.S.C. § 1964(c).

COUNT TWO (all Defendants)
Conspiracy to Violate RICO Statute, 18 U.S.C. § 1962(d)

272. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

273. The RICO Act provides that "[i]t shall be unlawful for any person to conspire to violate any of the provisions" of the Act. 18 U.S.C. § 1962(d).

274. Defendants and other members of the Qatari Enterprise knowingly and willfully agreed to facilitate, participate in, manage, and direct an enterprise that would affect interstate commerce through a pattern of racketeering activity. They shared the common objective of conducting the Qatari Enterprise through a pattern of racketeering.

275. Defendants have committed overt acts in furtherance of the conspiracy. Defendant Muzin has stated that, at times relevant to this Complaint, he and other agents of Qatar had regular meetings at the Qatari Embassy, during which they discussed "hurdles" to Qatar's goals of easing sanctions and improving its diplomatic standing. Muzin confirmed that he specifically identified Mr. Broidy as one such obstacle, and that Mr. Broidy was therefore "in danger."

276. On information and belief, Defendants agreed with other members of the Qatari Enterprise during one or several of their meetings, and at other times, to engage in the above-mentioned racketeering actions to harm Mr. Broidy's business and standing in the community.

277. Defendants and other members of the Qatari Enterprise committed the above-referenced racketeering acts in furtherance of their racketeering conspiracy.

278. As a direct consequence and by reason of Defendants' racketeering conspiracy, Plaintiffs have suffered injury, which includes, but is not limited to, damage resulting from loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; loss in the value of

Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial. Plaintiffs are entitled to treble damages and attorneys' fees under 18 U.S.C. § 1964(c).

COUNT THREE (all Defendants)
Stored Communications Act
18 U.S.C. §§ 2701 *et seq.*

279. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

280. The Stored Communications Act imposes criminal penalties on "whoever . . . intentionally accesses without authorization a facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(1).

281. The Act also provides that "a person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity" damages, along with equitable and declaratory relief. 18 U.S.C. § 2707.

282. Plaintiffs are "persons" within the meaning of 18 U.S.C. §§ 2510(6) and 2707(a).

283. Defendants conspired with persons who willfully and intentionally accessed without authorization a facility through which an electronic communication service is provided, namely, BCM's computer systems, including its email servers, as well as Google's servers, thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a).

284. The cyberattack was a willful, flagrant, and intentional violation of the Stored Communications Act. The hackers used VPN and other tools to mask their cyber intrusions and avoid detection, thereby showing sophistication and consciousness of guilt. Defendants unlawfully conspired with persons who, unlawfully and without authorization accessed

Plaintiffs' computer systems and email servers thousands of times over a period of almost two months, in a sustained cyberattack.

285. As a result of Defendants' conduct, Plaintiffs have suffered damages, including, but not limited to, loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial. As provided for in 18 U.S.C. § 2707, Plaintiffs are entitled to an award of the greater of the actual damages suffered or the statutory damages, punitive damages, attorneys' fees and other costs of this action, and appropriate equitable relief.

286. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in any further cyberattacks or committing the conduct described in this Cause of Action.

COUNT FOUR (all Defendants)
Computer Fraud and Abuse Act
18 U.S.C. § 1030(a)(2) and (a)(5)

287. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

288. The Computer Fraud and Abuse Act creates a cause of action against whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2).

289. The Act also creates a cause of action against whoever "(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally

accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss." 18 U.S.C. § 1030(a)(5).

290. The Act also creates a cause of action against "[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section." 18 U.S.C. § 1030(b).

291. A "protected computer" is one that "is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).

292. BCM's computer systems and email servers are used in and affect interstate and foreign commerce or communication and are therefore "protected computers."

293. Defendants conspired with others to intentionally, unlawfully and without authorization access Plaintiffs' computer systems and email servers thousands of times over a period of almost two months, in a sustained cyberattack. Defendants intentionally conspired to cause damage to BCM's protected computers through the attack.

294. Defendants conspired with others who intentionally accessed or caused to be accessed Plaintiffs' servers, and emails and documents physically located on those servers, at BCM's offices, as well as Google servers, specifically by accessing or causing to be accessed accounts associated with Mr. Broidy and other BCM employees.

295. The hackers accessed "protected computers," defined by 18 U.S.C. § 1030(e)(2)(B) as computers "used in or affecting interstate or foreign commerce or communication." They knowingly caused the transmission of a program, information, code, or command, and as a result, intentionally causes damage without authorization, to BCM's protected computers.

296. The hackers willfully and intentionally accessed the email accounts of, at least, Robin Rosenzweig and Mr. Broidy's Executive Assistant by transmitting fake spear phishing emails that stole their login credentials, and thereafter, beginning on or about January 16, 2018, accessed BCM's servers without authorization. They accessed emails and documents physically located on those servers, including the accounts of Mr. Broidy and other BCM employees.

297. The hackers also implemented identifiable obfuscation techniques, such as VPN, to engage in ultimately unsuccessful efforts to hide the origin of their spear phishing attacks and unauthorized access to Plaintiffs' servers, and emails and documents physically located on those servers and the servers of Google.

298. As a direct and proximate result of the actions of Defendants and their co-conspirators, Plaintiffs suffered damage, including harm to the integrity and availability of their servers, and to emails and documents physically located on those servers.

299. As a direct and proximate result of the actions of Defendants and their co-conspirators, Plaintiffs also suffered loss, including, but not limited to, damages resulting from loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; the investigation costs associated with identifying the cyber-attacks and repairing the integrity of Plaintiffs' servers after the attacks, including by hiring forensic investigators and data security experts, and attorneys, among other losses, in an amount to be proven at trial, but in any event, in excess of $75,000, exclusive of interest and costs.

300. Defendants intentionally and willfully caused such damage to Plaintiffs.

301. Defendants' conduct has caused, and will continue to cause Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased

risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in the conduct described in the Cause of Action.

COUNT FIVE (all Defendants)
Misappropriation of Trade Secrets
(18 U.S.C. §§ 1831, 1832, 1836)

302. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

303. Federal law creates a cause of action against "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains" trade secrets. 18 U.S.C. § 1832(a)(1).

304. Federal law imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). *See* § 1832(a)(5).

305. Federal law also creates a cause of action against "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret." 18 U.S.C. § 1831(a)(1).

306. Federal law imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" the offense listed in § 1831(a)(1). *See* § 1831(a)(5).

307. "An owner of a trade secret that is misappropriated may bring a civil action. . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1).

308. The BCM server stored trade secrets including but not limited to highly confidential business plans and proposals, research supporting those plans and proposals including costs and service projections, information concerning business strategies and opportunities, and contacts for important business relationships. These trade secrets are of substantial value to Plaintiffs, as will be proven at trial.

309. BCM stored trade secrets that were used in interstate and foreign commerce. Plaintiffs have taken and continue to take reasonable measures to keep this information secret. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

310. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

311. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

312. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

313. Defendants unlawfully conspired to take, appropriate, and obtain Plaintiffs' trade secrets without authorization, by means of a cyberattack against Plaintiffs. Defendants knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs.

314. Defendants improperly disclosed and misappropriated Plaintiffs' trade secrets without consent or authorization when they widely disseminated those trade secrets to fellow members of the Qatari Enterprise and to media organizations for publication; at the time of such

disclosure, Defendants knew or had reason to know that the information disclosed consisted of trade secrets.

315. Defendants misappropriated Plaintiffs' trade secrets intentionally for the benefit their foreign client, Qatar, and acted with the knowledge that their actions would have the effect of benefiting the foreign government of Qatar.

316. As a direct consequence of Defendants' actions, Plaintiffs have suffered damages, which include, but are not limited to, loss of consumer goodwill, loss in the value of Plaintiffs' trade secrets and confidential business information, and harm to Plaintiffs' business, in an amount to be proven at trial. *See* 18 U.S.C. § 1836(b)(3)(B)(i)(I). Defendants' acts of misappropriation have affected interstate commerce.

317. As a direct consequence of Defendants' unlawful actions, Defendants have unjustly benefited from their possession of Plaintiffs' trade secrets. Defendants were paid money from the Qatari Enterprise to conspire to steal and misappropriate Plaintiffs' trade secrets. Plaintiffs seek damages in the amount of that unjust enrichment, and disgorgement of Defendants' profits pursuant to 18 U.S.C. § 1836(b)(3)(B)(i)(II).

318. Defendants' conduct was willful and malicious, and thus Plaintiffs are entitled to exemplary damages pursuant to 18 U.S.C. § 1836(b)(3)(C), equal to twice the amount of their proven damages. Plaintiffs are also entitled to attorneys' fees pursuant to 18 U.S.C. § 1836(b)(3)(C).

319. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages.

Plaintiffs accordingly seek an injunction prohibiting Defendants from misappropriating its trade secrets or engaging in any other conduct described in this Cause of Action.

320. Defendants' conduct constitutes criminal conduct in violation of 18 U.S.C. §§ 1831 and 1832. As such, it constitutes predicate racketeering activity under the Racketeer Influenced and Corrupt Organizations ("RICO") Act, 18 U.S.C. § 1962.

COUNT SIX (all Defendants)
Misappropriation of Trade Secrets
Uniform Trade Secrets Act
Cal. Civ. Code § 3426 *et seq.*

321. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

322. The law of the State of California provides a cause of action for damages and injunctive relief in response to the misappropriation of trade secrets. Cal. Civ. Code §§ 3426.2 3426.3.

323. Defendants misappropriated a "trade secret" as defined by Cal. Civ. Code § 3426.1 to include "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

324. The BCM server stored trade secrets, including but not limited to highly confidential business plans and proposals, research supporting those plans and proposals including costs and service projections, information concerning business strategies and opportunities, and contacts for important business relationships. These trade secrets are of substantial value to Plaintiffs, as will be proven at trial.

325. Plaintiffs take and have taken reasonable measures to keep this information secret. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

326. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

327. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

328. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

329. Defendants improperly disclosed and misappropriated Plaintiffs' trade secrets without consent or authorization when they widely disseminated those trade secrets to fellow members of the Qatari Enterprise and to media organizations for publication; at the time of such disclosure, Defendants knew or had reason to know that the information disclosed consisted of trade secrets.

330. As a direct consequence of Defendants' actions, Plaintiffs have suffered damages, which include, but are not limited to, damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets and business information, and other intellectual property; costs expended in protecting trade secrets from future misappropriation; and harm to Plaintiffs' business, in an amount to be proven at trial.

331. As a direct consequence of Defendants' unlawful misappropriation of Plaintiffs' trade secrets, Defendants have unjustly profited from their possession of Plaintiffs' trade secrets. Defendants were paid money from the Qatari Enterprise to steal and misappropriate Plaintiffs'

trade secrets. Plaintiffs seek damages in the amount of that unjust enrichment, and disgorgement of Defendants' profits.

332. Defendants' conduct was willful and malicious, and thus Plaintiffs are entitled to exemplary damages pursuant to Cal. Civ. Code § 3426.3, equal to twice the amount of their proven damages. Plaintiffs are also entitled to attorneys' fees pursuant to Cal. Civ. Code § 3426.4.

333. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from misappropriating its trade secrets or engaging in any other conduct described in this Cause of Action.

COUNT SEVEN (all Defendants)
Receipt and Possession of Stolen Property
in Violation of Cal. Pen. Code § 496

334. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

335. California law imposes criminal penalties on any "person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained." Cal. Penal Code § 496(a).

336. California law further provides that "[a]ny person who has been injured by a violation of [Section 496] may bring an action for three times the amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney's fees."

337. Defendants conspired with others to hack into Plaintiffs' computer systems and email services located in California.

338. Defendants knowingly received property, including private communications, documents, trade secrets and intellectual property housed on Plaintiffs' and Google's servers, and in emails and documents physically located on those servers located in California.

339. This property was stolen from Plaintiffs in California or otherwise obtained from Plaintiffs in California in a manner that constitutes theft.

340. Defendants received the property knowing that it was stolen property and obtained through theft. They knowingly and intentionally concealed, sold, withheld—and aided in concealing, selling, and withholding of—Plaintiffs' stolen property.

341. As a result of Defendants' actions, Plaintiffs suffered damages including, but not limited to, damages resulting from loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial.

342. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction to return Plaintiffs' stolen property and to refrain from engaging in any conduct described in this Cause of Action.

COUNT EIGHT (all Defendants)
California Comprehensive Computer Data Access and Fraud Act
Cal. Pen. Code § 502

343. California law imposes criminal penalties on anyone who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Cal. Penal Code § 502(c)(2).

344. California law imposes criminal penalties on anyone who "[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network." Cal. Penal Code § 502(c)(4).

345. California law imposes criminal penalties on anyone who "[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of" Section 502. Cal. penal Code § 502(c)(6).

346. California law imposes criminal penalties on anyone who "[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. § 502(c)(7).

347. California law imposes criminal penalties on anyone who "[k]nowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network." Cal. Penal Code § 502(c)(9).

348. California law provides that "the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator

for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." Cal. Penal Code § 502(e)(1).

349. California law provides for award of reasonable attorneys' fees. Cal. Penal Code § 502(e)(2).

350. Defendants knowingly and unlawfully conspired with others to access computers, computer systems or computer networks at Plaintiff BCM and Google, all of which were located in California. Defendants knew that at the time that they did not have the authorization to access Plaintiffs' computers, computer systems, and networks. This knowledge is demonstrated by conspirators' use of spear phishing attacks and attempted spear phishing attacks to disguise their intentions and obtain login credentials through fraudulent misrepresentations. The spear phishing emails imitated Google's profile in order to obtain login credentials. Hackers conspiring with Defendants caused damage to Plaintiffs electronic files and emails through their cyber intrusions.

351. As a result of Defendants' actions, Plaintiffs suffered damages including, but not limited to, damages resulting from loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; substantial costs to assess and restore server and digital system security and operations; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial.

352. Defendants' actions were willful and malicious, and Plaintiffs are entitled to punitive damages under § 502(e)(4).

353. Defendants' actions have caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction to refrain from engaging in any conduct described in this Cause of Action.

COUNT NINE (all Defendants)
Public Disclosure of Private Facts

354. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

355. Plaintiffs have a legally protected privacy interest in their personal information. This includes their Google login information, their emails, and documents contained on BCM's servers and computer systems.

356. Defendants conspired with persons to purposefully and repeatedly hack Plaintiffs' computer systems and email servers over a period of weeks, with thousands of instances of unauthorized access, including from locations within the United States. They then published the information they illegally obtained or fabricated during the cyberattack. They did so without permission and with specific intent to access and obtain Plaintiffs' personal and private information.

357. Defendants' publicized the illegally obtained information in phone calls and other communications with journalists and media organizations in March of 2017 and other times within a year of the commencement of this action.

358. Much of the information Defendants illegally obtained in the hacking concerned Mr. Broidy's private matters and is not of public interest. Defendants' tortious scheme—using repeated cyber crime to publish secrets of a private citizen—is highly offensive and shocking to

any reasonable person. Defendants were retained specifically as part of an effort to ruin Mr. Broidy's public standing. They accomplished that end through illegal means, by stealing and publishing private facts about his personal life and confidential business matters.

359. The public disclosure of Plaintiffs' personal information has caused, and will continue to cause, Plaintiffs injury, including an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money, and effort safeguarding their personal information in the wake of these series of hacks.

360. Plaintiffs will continue to suffer this injury as long as their personal information is available to Defendants and, subsequently, to media organizations and the world at large.

361. The public disclosure of Plaintiffs' personal information has also caused them to suffer monetary damages, at an amount to be proven at trial, but in any event, in excess of $75,000, exclusive of interest and costs. Because Defendants' actions are intolerable in a civilized community and must be deterred, Plaintiffs also seek punitive damages.

362. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from violating Plaintiffs' privacy or engaging in the conduct described in this Cause of Action.

COUNT TEN (all Defendants)
Intrusion Upon Seclusion

363. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

364. Plaintiffs have a legally protected privacy interest in their personal information. This includes their Google login information, their emails, and documents contained on BCM's

servers and computer systems. Plaintiffs' email servers and computer systems contained private information and secrets that Plaintiffs had secluded away from public attention and prying eyes.

365. Defendants conspired with others to purposefully and repeatedly hack Plaintiffs' computer systems and email servers over a period of weeks. In so doing, they intruded upon Plaintiffs' secluded documents and private communications, viewing them through electronic means and then printing them out.

366. Much of the information Defendants illegally obtained in the hacking concerned Mr. Broidy's private matters and is not of public interest. Defendants' tortious scheme—using repeated cyber crime to publish secrets of a private citizen—is highly offensive and shocking to any reasonable person. Defendants were retained specifically as part of an effort to harm Mr. Broidy's business and public standing. They accomplished that end through illegal means, by stealing and publishing private facts about his personal life and matters.

367. Hackers intruded upon Mr. Broidy's seclusion between January 16 and February 25, 2017, and other times within a year of the commencement of this action.

368. The public disclosure of misleading and curated information has caused Plaintiffs to suffer monetary damages, at an amount to be proven at trial, but in any event, in excess of $75,000, exclusive of interest and costs. The injury to Plaintiffs' privacy is ongoing, and thus the damages Plaintiffs seek may not be finally set. Because Defendants' actions are intolerable in a civilized community, Plaintiffs also seek punitive damages to deter this sort of criminal enterprise behavior.

369. The public disclosure of Plaintiffs' personal information has caused, and will continue to cause, Plaintiffs irreparable injury, including an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money,

and effort safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to Defendants and, subsequently, to media organizations and the world at large. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from violating Plaintiffs' privacy or engaging in the conduct described in this Cause of Action.

COUNT ELEVEN (all Defendants)
Conversion

370. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

371. Plaintiffs had ownership of and the right to possess their property, including their login credentials, emails, private communications, business documents, trade secrets and intellectual property.

372. By appropriating Plaintiffs' login credentials, hackers, acting as members of a Defendants' civil conspiracy and criminal enterprise, unlawfully exercised ownership, dominion, and control over Plaintiffs' property. They stole a vast amount of valuable electronic information from Plaintiffs' computer systems and email servers, and used them to create PDF and hard-copy documents that they then disseminated to media organizations. Some members of the criminal enterprise, having received stolen property, continued to own and control it, in violation of California Penal Code § 496. Defendants continue to control and disseminate Plaintiffs' emails, electronic communications, business documents, contracts, and intellectual property—included copyrighted materials and trade secrets—and thereby still deny Defendants their lawful dominion, ownership, and control over that property.

373. Defendants' conversion of Plaintiffs' property has caused Plaintiffs to suffer monetary damages, at an amount to be proven at trial, but in any event, in excess of $75,000, exclusive of interest and costs. Plaintiffs' damages include, but are not limited to, damages resulting from injury to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial. The injury to Plaintiffs is ongoing, and thus the damages Plaintiffs seek are not yet set. Because Defendants' actions are intolerable in a civilized community, Plaintiffs also seek punitive damages to deter this sort of criminal enterprise behavior.

374. Defendants' massive conversion of such a large amount of Plaintiffs' property has caused, and will continue to cause, Plaintiffs injury, including loss of consumer goodwill, and an increased risk of harassment. Such irreparable harm cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from converting or stealing any of Plaintiffs' property, as described in this Cause of Action. Plaintiffs further demand an order requiring Defendants return all stolen property belonging to Plaintiffs immediately upon this Court's order.

COUNT TWELVE (all Defendants)
Tortious Interference

375. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

376. Defendants tortiously interfered with Plaintiffs' business relationships. The Qatari Enterprise attempted for years to interfere with Mr. Broidy's business as a means of intimidating him from criticizing Qatar and its regime's sponsorship of terrorism.

377. Defendants conspired with persons to hack Plaintiffs' emails, contracts, and other business documents, and then disseminated carefully curated versions of documents to falsely and misleadingly connect Mr. Broidy to wrongdoing. These actions tortiously harmed Plaintiffs' business relationships. Defendants acted knowingly with the specific intent of harming Mr. Broidy's business relationships by falsely associating him with illegal activity in order to silence his criticism of Qatar.

378. In particular, Defendants sought to harm Mr. Broidy's relationships with Jewish clients, in order to diminish his influence in opposing Qatar's sponsorship of terrorism. Plaintiffs represent that they will be able to prove at trial that their business relationships has suffered material harm, amounting to breach or non-performance of contract, since the Qatari Enterprise began its tortious scheme, and Plaintiffs were forced to forego business opportunities due to the fallout from the cyberattack.

379. Defendants' numerous acts of tortious interference with Plaintiffs' business relationships have caused Plaintiffs to suffer monetary damages, at an amount to be proven at trial, but in any event, in excess of $75,000, exclusive of interest and costs. Damages include, but are not limited to, damages resulting from injury to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial. The tortious interference is ongoing, because Defendants are still using the property they fraudulently obtained to harm Plaintiffs' business relationships, and thus the damages Plaintiffs seek are not yet set. Because Defendants' actions are intolerable in a civilized community, Plaintiffs also seek punitive damages to deter this sort of criminal enterprise behavior.

380. Defendants' tortious interference has caused, and will continue to cause, Plaintiffs injury, including loss of consumer goodwill, and an increased risk of harassment. Such irreparable harm cannot be compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in any further tortious interference against Plaintiffs or their business relationships.

COUNT THIRTEEN (all Defendants)
Civil Conspiracy

381. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

382. Defendant Muzin has stated that, at times relevant to this Complaint, he and other agents of Qatar had regular meetings at the Qatari Embassy, during which they discussed "hurdles" to Qatar's goals of easing sanctions and improving its diplomatic standing. Muzin confirmed that he specifically identified Mr. Broidy as one such obstacle, and that Mr. Broidy was therefore "in danger."

383. Defendants agreed during one or several of their meetings, and at other times, to engage in the above-mentioned tortious and criminal actions to harm Mr. Broidy's business and public standing.

384. Defendants willfully, intentionally, and knowingly agreed and conspired with each other and with others, including Qatar, to engage in the wrongful conduct alleged herein, including but not limited to:

a. Willfully and intentionally accessing without authorization a facility through which an electronic communication service is provided, namely, BCM's computer systems, including its email servers, and thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a);

b. Intentionally accessing Plaintiffs' and Google's servers, and emails and documents physically located on those servers and accounts, without

authorization and then stealing and curating Plaintiffs' data and emails, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) and Cal. Pen. Code § 502;

c. Willfully, intentionally, and maliciously misappropriating Plaintiffs' trade secrets to benefit the government of Qatar, a foreign power, in violation of both the laws of the United States and California;

d. Knowingly and intentionally receiving stolen property and concealing that property from Plaintiffs, in violation of California law;

e. Invading Plaintiffs' privacy by publicizing private facts and intruding upon his seclusion;

f. Taking and converting Plaintiffs' exclusive private and personal property without permission and with deliberate intent to access and obtain Plaintiffs' personal and private information; and

g. Tortiously interfering with Plaintiffs' business relationships by using documents and information stolen from Plaintiffs' servers to disparage Plaintiffs' business and conduct.

385. Defendants engaged in several overt acts to further and effectuate their conspiracy. Defendant Muzin admitted that he identified Mr. Broidy as a hindrance to Qatar's plans, knowing that this would prompt the conspiracy to harm Mr. Broidy and his business. All Defendants communicated with each other before, during, and after the above-referenced cyberattacks in order to effectuate the conspiracy. They knowingly provided media organizations, public relations professionals, and other Qatari agents with information stolen and carefully curated from the hackings in order to harm Plaintiffs. Defendants attempted to conceal their illegal conspiracy by falsifying or failing to file their FARA disclosures. These and other overt acts are reasonably certain to be proven at trial.

386. Each Defendant actively participated in the above-described civil conspiracy, and therefore each Defendant is responsible for each tortious and otherwise illegal action of any co-conspirator.

387. As a direct consequence of Defendants' conspiracy, Plaintiffs have suffered monetary damages, at an amount to be proven at trial, but in any event in excess of $75,000, exclusive of interest and costs, which include, but are not limited to, damages resulting from injury to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial.

388. This conspiracy is ongoing. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from misappropriating its trade secrets or engaging in any other conduct described in this Cause of Action.

PRAYER FOR RELIEF

389. Plaintiffs repeat and re-allege the allegations contained in each and every preceding paragraph of this Complaint.

390. Wherefore, Plaintiffs request that this Court order the following relief:

a. Grant judgment in favor of Plaintiffs and against Defendants as to all Causes of Action;

b. Declare that Defendants' conduct constitutes violations of the statutes and common law cited herein;

c. Award Plaintiffs an appropriate amount in monetary damages as determined at trial, including pre- and post-judgment interest and treble damages under RICO, 18 U.S.C. § 1964 and Cal. Pen. Code § 496;

d. Grant all appropriate injunctive relief, disgorgement of unjust riches, constructive trust over Plaintiffs' trade secrets and other materials, and any other equitable relief deemed appropriate;

e. Award Plaintiffs punitive damages under 18 U.S.C. § 2707, and Cal. Pen. Code § 502, and Plaintiffs' common-law causes of action, as well as exemplary damages under Cal. Civ. Code § 3426.3, and 18 U.S.C. § 1836(b)(3)(C);

f. Award Plaintiffs attorneys' fees and the costs of bringing this action; and

g. Grant Plaintiffs such other relief as is just and appropriate.

JURY DEMAND

Plaintiffs hereby demand a trial by jury.

Respectfully Submitted,

/s/ Filiberto Agusti
Filiberto Agusti (DC Bar No. 270058)
Shannen W. Coffin (DC Bar No. 449197)
Michael J. Baratz (DC Bar No. 480607)
STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Phone: (202) 429-3000
Fax: (202) 429-3902
FAgusti@steptoe.com
scoffin@steptoe.com
mbaratz@steptoe.com

Counsel for Plaintiffs Broidy Capital Management and Elliott Broidy

Dated: January 24, 2019